T.C.
TRAKYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ÜNİVERSİTE ÖĞRENCİLERİNİN DİJİTAL VERİ GÜVENLİĞİ FARKINDALIKLARININ DİJİTAL VATANDAŞLIK BAĞLAMINDA İNCELENMESİ

MERT HIZMALI

YÜKSEK LİSANS TEZİ

BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ ANABİLİM DALI

Tez Danışmanı: Doç. Dr. Nilgün TOSUN

EDİRNE-2022

Mert HIZMALI'nın hazırladığı **"ÜNİVERSİTE ÖĞRENCİLERİNİN DİJİTAL VERİ GÜVENLİĞİ FARKINDALIKLARININ DİJİTAL VATANDAŞLIK BAĞLAMINDA İNCELENMESİ"** başlıklı bu tez tarafımızca okunmuş, kapsam ve niteliği açısından Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalında bir **Yüksek lisans** tezi olarak kabul edilmiştir.

Jüri Üyeleri:	İmza
Doç. Dr. Nilgün TOSUN (Danışman)	……
Doç. Dr. Fatma AKGÜN	……
Dr. Öğr. Üy. Zerrin AYVAZ REİS	……

Tez Savunma Tarihi: 07/07/2022

Bu tezin Yüksek Lisans tezi olarak gerekli şartları sağladığını onaylarım.

İmza

Doç. Dr. Nilgün TOSUN
Tez Danışmanı ……

Trakya Üniversitesi Fen Bilimleri Enstitüsü onayı

…..……...
Prof. Dr. Hüseyin Rıza Ferhat KARABULUT
Fen Bilimleri Enstitüsü Müdürü

T.Ü. FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ ANABİLİM DALI YÜKSEK LİSANS PROGRAMI DOĞRULUK BEYANI

Trakya Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında, tüm verilerin bilimsel ve akademik kurallar çerçevesinde elde edildiğini, kullanılan verilerde tahrifat yapılmadığını, tezin akademik ve etik kurallara uygun olarak yazıldığını, kullanılan tüm alan yazın bilgilerinin bilimsel normlara uygun bir şekilde kaynak gösterilerek ilgili tezde yer aldığını ve bu tezin tamamı ya da herhangi bir bölümünün daha önceden Trakya Üniversitesi ya da farklı bir üniversitede tez çalışması olarak sunulmadığını beyan ederim.

07 / 07 / 2022
Mert HIZMALI

Yüksek Lisans Tezi
Üniversite Öğrencilerinin Dijital Veri Farkındalıklarının Dijital Vatandaşlık Bağlamında İncelenmesi
T.Ü. Fen Bilimleri Enstitüsü
Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı

ÖZET

Bu çalışmada, üniversite öğrencilerinin dijital veri güvenliği farkındalıkları dijital vatandaşlık bağlamında incelenmiştir. Çalışmanın amacı; üniversite öğrencilerinin dijital veri güvenliği farkındalıkları ile dijital vatandaşlık düzeylerinin demografik değişkenler açısından incelenmesi ve bu iki kavram arasındaki ilişkinin ortaya konmasıdır. Bu amaç doğrultusunda öncelikle üniversite öğrencilerinin dijital veri güvenliği farkındalığı ve dijital veri güvenliği düzeyleri cinsiyet, öğrenim görmekte olduğu eğitim kademesi, sınıf düzeyi, günlük ortalama internet kullanma süresi ve ailenin aylık ortalama gelir düzeyi değişkenleri açısından incelenmiştir. Çalışmaya Trakya Üniversitesi'nin ön lisans, lisans ve lisansüstü kademelerinde öğretim gören 2500 öğrenci gönüllü olarak katılmıştır. Araştırma verileri üç bölümden oluşan anket formu ile toplanmıştır. Formun birinci bölümünde araştırmacı tarafından hazırlanan kişisel bilgileri içeren sorular, ikinci bölümünde Som-Vural (2016) tarafından geliştirilen Dijital Vatandaşlık Ölçeği ve üçüncü bölümünde ise Yılmaz ve diğerleri (2015) tarafından geliştirilen Dijital Veri Güvenliği Farkındalığı Ölçeği yer almaktadır. Veriler katılımcılardan sınıf ortamında yüz yüze toplanmıştır. Elde edilen verilerin istatiksel analizi SPSS 25.0 programı ile yapılmıştır. Analizler sonucunda üniversite öğrencilerinin genelinin dijital vatandaşlık düzeyinin ve dijital veri farkındalığının yüksek olduğu saptanmıştır. Katılımcıların dijital veri güvenliği farkındalığı ve dijital vatandaşlık düzeyleri arasında yüksek düzeyde pozitif anlamlı bir ilişki olduğu görülmüştür. Erkek öğrencilerin kadınlara göre dijital vatandaşlık ve dijital veri güvenliği puanlarının daha yüksek olduğu, dijital vatandaşlık ve dijital veri güvenliği farkındalık puan ortalamalarının lisans öğrencilerinin ön lisans öğrencilerinden daha yüksek olduğu, yüksek lisans/doktora öğrencilerinin ise yakın bir

ortalamaya sahip olduğu görülmüştür. Lisans ve yüksek lisans/doktora öğrencilerinin vatandaşlık ve dijital veri güvenliği farkındalığı puanlarının ön lisans öğrencilerinden daha yüksek olduğu, lisans ve yüksek lisans/doktora öğrencileri arasında ise farklılık olmadığı belirlenmiştir. Sınıf düzeylerine göre dijital vatandaşlık ortalamaları incelendiğinde sınıf düzeyi arttıkça ortalamanın da arttığı, dijital veri güvenliği farkındalık ortalamalarının sınıf düzeyine göre arttığı, farklılığın ise istatistiksel olarak anlamlı olmadığı belirlenmiştir. Ailenin gelir düzeyi arttıkça dijital vatandaşlık puan ortalaması da artmaktadır.

Yıl **:** 2022

Sayfa Sayısı **:** 126

Anahtar Kelimeler: Dijital Vatandaşlık, Dijital Veri Güvenliği, Üniversite Öğrencileri

Master's Thesis

Investigation of Digital Data Awareness of University Students in the Context of Digital Citizenship

Trakya University Institute of Natural and Applied Sciences

Department of Computer Education and Instructional Technology

ABSTRACT

In this study, digital data security awareness of university students was examined in the context of digital citizenship. The aim of the study; The aim of this study is to examine the digital data security awareness and digital citizenship levels of university students in terms of demographic variables and to reveal the relationship between these two concepts. For this purpose, first of all, university students' digital data security awareness and digital data security levels were examined in terms of gender, education level, class level, average daily internet usage time and monthly average income level of the family. 2500 students studying at the associate, undergraduate and graduate degrees of Trakya University voluntarily participated in the study. Research data were collected with a questionnaire consisting of three parts. The first part of the form includes questions containing personal information prepared by the researcher, the second part includes the Digital Citizenship Scale developed by Som-Vural (2016), and the third part includes the Digital Data Security Awareness Scale developed by Yılmaz et al. (2015). The data were collected from the participants face to face in the classroom environment. Statistical analysis of the obtained data was done with SPSS 25.0 program. As a result of the analyzes, it was determined that the digital citizenship level and digital data awareness of the university students in general were high. It was observed that there was a high level of positive and significant relationship between the digital data security awareness and digital citizenship levels of the participants. It has been seen that male students have higher digital citizenship and digital data security scores than females, digital citizenship and digital data security awareness averages are higher than undergraduate students'

associate degree students, and graduate/doctorate students have a close average. It was determined that the citizenship and digital data security awareness scores of undergraduate and graduate/doctorate students were higher than those of associate degree students, and there was no difference between undergraduate and graduate/doctorate students. When the digital citizenship averages according to the class levels were examined, it was determined that the average increased as the class level increased, the digital data security awareness averages increased according to the class level, and the difference was not statistically significant. As the income level of the family increases, the digital citizenship score average also increases.

Year : 2022

Number of pages : 126

Keywords: Digital Citizenship, Digital Data Security, University Students

TEŞEKKÜR

Bu çalışmanın gerçekleşmesinde iki dönem boyunca değerli bilgilerini benimle paylaşan, hayatıma kattığı önemini asla unutmayacağım danışmanım Doç. Dr. Nilgün TOSUN'a çok teşekkür ederim.

Maddi destek vererek tezimin projelendirilmesini sağlayan (2022/73 nolu proje) Trakya Üniversitesi Rektörlüğü'ne ve İdari ve Mali İşler Daire Başkanlığı Bilimsel Araştırma Projeleri Birimi'ne çok teşekkür ederim.

Yüksek lisans eğitimime başlamadan önce ve başladıktan sonra süreç boyunca benden yardımlarını ve desteklerini esirgemeyen annem Filiz HIZMALI, babam Ahmet HIZMALI ve kız kardeşim Merve HIZMALI'ya teşekkürlerimi sunarım.

İÇİNDEKİLER

ÖZET iv
ABSTRACT vi
TEŞEKKÜR viii
İÇİNDEKİLER ix
SİMGELER VE KISALTMALAR DİZİNİ xi
ÇİZELGELER DİZİNİ xii
ŞEKİLLER DİZİNİ xiii
BÖLÜM 1 1
GİRİŞ 1
1.1. Araştırmanın Problemi 1
1.2. Tezin Amacı ve Önemi 3
1.3. Sayıltılar 4
1.4. Sınırlılıklar 4
BÖLÜM 2 5
KAVRAMSAL ÇERÇEVE VE İLGİLİ ARAŞTIRMALAR 5
2.1. Dijital Vatandaşlık 5
2.1.1. Dijital Vatandaşlığın Boyutları 7
2.1.2. Dijital Vatandaşlık Farkındalığı Konusunda Türkiye'de Yapılan Çalışmalar 18
2.1.3. Dijital Vatandaşlık Farkındalığı Konusunda Dünyada Yapılan Çalışmalar 24
2.2. Dijital Veri 26
2.2.1. Dijital Veri Güvenliği 27
2.3. Türkiye'de Yapılan Akademik Çalışmalar 42
2.3.1. Dijital Vatandaşlık ile İlgili Akademik Çalışmalar 42
2.3.2. Dijital Veri Güvenliği Farkındalığı ile İlgili Yapılan Çalışmalar 46
2.4. Yurtdışında Yapılan Akademik Çalışmalar 49

2.4.1. Dijital Vatandaşlık ile İlgili Akademik Çalışmalar 49
2.4.2. Dijital Veri Güvenliği Farkındalığı ile İlgili Yapılan Çalışmalar 52
BÖLÜM 3 56
YÖNTEM 56
3.1. Araştırmanın Modeli 56
3.2. Çalışma Grubu 56
3.2. Veri Toplama Araçları 58
3.3. Verilerin Toplanması 62
3.4. Verilerin Analizi 62
BÖLÜM 4 63
BULGULAR 63
4.1. Dijital Veri Güvenliği Farkındalığına Dair Bulgular 63
4.2. Dijital Vatandaşlığa Dair Bulgular 68
4.3. Dijital Veri Güvenliği Farkındalığı ve Dijital Vatandaşlık Arasındaki İlişkiye Dair Bulgular 73
BÖLÜM 5 74
TARTIŞMA 74
BÖLÜM 6 85
SONUÇ VE ÖNERİLER 85
KAYNAKLAR 88
EK 1: Kişisel Bilgi Soruları 100
EK 2: Dijital Vatandaşlık Ölçeği 102
EK 3: Dijital Vatandaşlık Ölçek Kullanım İzni 105
EK 4: Dijital Veri Güvenliği Ölçeği 105
EK 5: Dijital Veri Güvenliği Ölçek Kullanım İzni 109
EK 6: Etik Kurul Onayı 110
ÖZGEÇMİŞ 113

SİMGELER VE KISALTMALAR DİZİNİ

AB : Avrupa Birliği

BDDK : Bankacılık Düzenleme ve Denetleme Kurumu

BÖTE : Bilgisayar ve Öğretim Teknolojileri Eğitimi

BT **:** Bilişim Teknolojileri

ISTE :The International Society for Technology in Education (Uluslararası Eğitimde Teknoloji Topluluğu)

KVKK : Kişisel Verileri Koruma Kanunu

MEB : Milli Eğitim Bakanlığı

SIEM : Security Information and Event Management (Güvenlik Bilgileri ve Olay Yönetimi)

TBMM : Türkiye Büyük Millet Meclisi

TÜİK : Türkiye İstatistik Kurumu

YÖK : Yüksek Öğretim Kurumu

ÇİZELGELER DİZİNİ

Çizelge 2.1. Bireylerin İnternet Kullanım Sıklığı 2020-2021……..10

Çizelge 3.1. Katılımcıların Demografik Bilgileri…….55

Çizelge 3.2. Teknolojik Cihaz Sahipliği Durumu……56

Çizelge 4.1. Çalışma Grubunun Dijital Veri Güvenliği Farkındalıklarına Ait Betimsel İstatistikleri…….62

Çizelge 4.2. Dijital Veri Güvenliği Farkındalık Puanlarının Cinsiyete Göre t Testi Sonuçları……..63

Çizelge 4.3. Öğrenim Görmekte Olduğu Eğitim kademesi, Sınıf düzeyi, Günlük Ortalama İnternet Kullanma Süresi ve Ailenin Aylık Ortalama Gelir Düzeyi Değişkenlerine Ait Betimsel İstatistikler……63

Çizelge 4.4. Öğrenim Görmekte Olduğu Eğitim Kademesi, Sınıf Düzeyi, Günlük Ortalama İnternet Kullanma Süresi ve Ailenin Aylık Ortalama Gelir Düzeyi Değişkenlerine Ait ANOVA Sonuçları……..65

Çizelge 4.5. Çalışma Grubunun Dijital Vatandaşlık Puanlarına Ait Betimsel İstatistikleri……..67

Çizelge 4.6. Dijital Vatandaşlık Puanlarının Cinsiyete Göre t Testi Sonuçları……67

Çizelge 4.7. Öğrenim Görmekte Olduğu Eğitim Kademesi, Sınıf Düzeyi, Günlük Ortalama İnternet Kullanma Süresi ve Ailenin Aylık Ortalama Gelir Düzeyi Değişkenlerine Ait Betimsel İstatistikler……68

Çizelge 4.8. Öğrenim Görmekte Olduğu Eğitim Kademesi, Sınıf Düzeyi, Günlük Ortalama İnternet Kullanma Süresi ve Ailenin Aylık Ortalama Gelir Düzeyi Değişkenlerine Ait ANOVA Sonuçları……..69

Çizelge 4.9. Dijital Vatandaşlık ve Dijital Veri Güvenliği Farkındalığı İlişkisi……71

ŞEKİLLER DİZİNİ

Şekil 2.1. Dijital Vatandaşlığın 4 Boyutu……7

Şekil 2.2. Dijital Vatandaşlığın 9 Boyutu……8

Şekil 2.3. İnternet Erişimi Olan Hanelerde ve Bireylerde İnternet Kullanım Oranı 2011-2021……10

Şekil 2.4. Dijital Vatandaşlığın 11 Boyutu……..17

Şekil 2.5. Hayat Eve Sığar Uygulaması……...18

Şekil 2.6. DQ World (Türkçe)…….20

Şekil 2.7. Çocukların İhtiyacı Olan 8 Temel DQ Vatandaşlık Becerisi……..20

Şekil 2.8. Bilinçli İnternet Hareketi Projesi…….21

Şekil 2.9. Fırsatları Artırma ve Teknolojiyi İyileştirme Hareketi……23

Şekil 2.10. Dijital Vatandaşlık Karikatür Yarışması…….....24

Şekil 2.11. EuroKids Online……....24

Şekil 2.12. Social Media Literacy for Change……..25

Şekil 2.13. Selma (Social and Emotional Learning for Mutual Awareness)……26

Şekil 3.1. Doğrulayıcı Faktör Analizi……..60

BÖLÜM 1

GİRİŞ

Bu bölümde; araştırmanın problemi, amacı ve önemi ile araştırmanın sayıltı ve sınırlılıklarına yer verilmiştir.

1.1. Araştırmanın Problemi

İnternet teknolojilerinde yaşanan gelişmelerle birlikte bireylerin yaşam biçimlerinde de belirgin değişimler olmuştur. Teknolojik gelişmeler sağlıktan eğitime, endüstriden iletişime kadar pek çok alanda etkisini göstermiştir. Alan yazında da teknolojik gelişmelere bağlı olarak yeni tanımlamalar ve terimler yapılmıştır (Yılmaz ve Doğusoy, 2020). Yeni terimler ve tanımlamalar arasında yer alan dijital vatandaşlık sıfatı da dijital ortamdaki eylemlerde etik davranmak, gereken güvenlik önlemlerini almak, olası olumlu veya olumsuz konulara karşı hazırlıklı olmak gibi dijital ortam kullanıcılarının dikkatli olması gereken konularda öne çıkan ve bunları yaşam biçimi olarak benimseyen bireyler için kullanılmaktadır (Som Vural ve Kurt, 2018). Ribble (2015) tarafından dijital vatandaşlık, teknolojinin uygun kullanımına ilişkin uygun davranış normları şeklinde ifade edilmektedir. Ribble (2011) tarafından dijital vatandaşlık; dijital ticaret, dijital erişim, dijital okuryazarlık, dijital hukuk, dijital iletişim, dijital etik, dijital hak ve sorumluluklar, dijital güvenlik ve dijital sağlık olarak dokuz boyutta ele alınmaktadır. Alberta Education (2012) ise bu boyutlara ek olarak dijital vatandaşlık politikaları ve bulut bilişim ile sahip olunan cihazlar boyutlarını ekleyerek dijital vatandaşlığın boyutlarının on bir olması gerekliliğini belirtmektedir. Dijital vatandaşların haber alma, iletişim kurma gibi temel olanaklardan faydalanma yanında üst düzey düşünme becerileri gerektiren yetkinliklere sahip olmaları da bir gerekliliktir (Som Vural ve Kurt, 2018).

Teknolojik gelişmeler ve yeni nesle yönelik çalışmalar eğitim- öğretim süreçlerinde araç ve uygulama bağlamında da değişimi gündeme getirmiştir. Odabaşı ve arkadaşları (2012) tarafından yeni teknolojilerle etkileşimde olan bir ortamda büyüyen öğrencilerin teknolojinin olduğu ortamlardan keyif aldıkları bildirilmektedir. Şahin (2009) tarafından yürütülmüş çalışmada ise değişen öğrenci profili ile eğitim sistemindeki öğrenci profiline ilişkin olarak yaşanan olanak uyuşmazlığının mevcut öğrencilere yaklaşıma ilişkin belirsizlik oluşturduğu bildirilmiştir. Ancak yeni nesil öğrencilerin son yıllarda dijital yaşamla sürekli etkileşimde olmalarından dolayı teknolojileri etkili, bilinçli ve güvenli kullanmaya ilişkin bilgi sahibi olmalarını da gerektirmektedir. Bu bağlamda son zamanlarda dijital güvenlik, dijital vatandaşlık, dijital veri güvenliği gibi terimler günlük hayatımıza girmiştir (Şahin, 2009).

Dijital teknolojilerin her geçen zamanda daha yoğun kullanılması dijital verilerin güvenliği probleminin gündeme gelmesine neden olmuştur. Veri güvenliği; gizlilik, bütünlük ve erişilebilirlik şeklinde üç boyutta ele alınabilmektedir. Diğer bir anlatımla verilerin başkaları tarafından görüntülenebilir olmaması, değiştirilebilir olmaması ile istenen mekân ve zamanda kullanıma hazır ulaşılabilir olması şeklinde ifade edilebilir (Kaya ve Öztürk, 2017).

Dijital vatandaşlık tanımlarında çevrimiçi ortama etkin katılım öne çıkan ortak noktalardan biridir. Bunun yanı sıra dijital vatandaşların bilgi iletişim teknolojileri kullanımlarının yasal, etik, sorumlu ve güvenli olduğu vurgulanmaktadır. Bilgi iletişim teknolojilerinin kullanımında bireylere maddi ya da manevi zarar verebilecek olan çok sayıda güvenlik tehdidi vardır (Çakır ve Kesler, 2012). Dijital veri güvenliğini tehdit eden bu unsurlar şifreleme araçları, kötücül yazılım temizleyici, saldırı tespit sistemleri, kablosuz ağ araçları, port tarayıcılar, güvenlik odaklı işletim sistemi gibi pek çok araç yardımıyla etkisiz hale getirilebilir (Baykara, Daş ve Karadoğan, 2013, s. 236). Bilgisayar ve iletişim ağlarının yoğun kullanımı ile birlikte teknolojik güvenlik ile dijital veri güvenliği önemini arttırmaya başlamıştır. Elektronik ortamda bilginin üretimi ve sunulması çeşitli avantajlar sağlamakla birlikte bazı güvenlik sorunlarına neden olmaktadır. Bireylerin bilgisayar sistemlerini kullanırken olası zararlardan korunmaları için tehlikelerin bilincinde olmaları önemli bir husustur.

Bu kapsamda; üniversite öğrencilerinin dijital vatandaşlık bağlamında dijital veri güvenliği farkındalığı düzeylerinin incelenmesine ilişkin yürütülecek bu tez çalışmasında problem cümlesi; "Üniversite öğrencilerinin dijital veri güvenliği farkındalığı ve dijital vatandaşlık düzeyleri, demografik özelliklere göre farklılık göstermekte midir?" şeklinde oluşturulmuştur.

1.2. Tezin Amacı ve Önemi

Tez çalışmasının amacı; üniversite öğrencilerinin dijital veri güvenliği farkındalıkları ile dijital vatandaşlık düzeylerinin belirlenmesi ve bu iki olgu arasındaki ilişkinin demografik değişkenler açısından incelenmesidir. Bu amaç doğrultusunda aşağıdaki sorulara yanıt aranacaktır:

1. Üniversite öğrencilerinin dijital vatandaşlık düzeyleri nedir?
2. Üniversite öğrencilerinin dijital veri güvenliği farkındalığı hangi düzeydedir?
3. Üniversite öğrencilerinin dijital veri güvenliği farkındalıkları ile dijital vatandaşlık düzeyleri arasında istatistiksel olarak anlamlı bir ilişki var mıdır?
4. Üniversite öğrencilerinin dijital veri güvenliği farkındalıkları;
    - Cinsiyet,
    - Öğrenim görmekte olduğu eğitim kademesi,
    - Sınıf,
    - Günlük ortalama internet kullanma süresi,
    - Teknolojik cihaz sahipliği,
    - Ailenin aylık ortalama gelir düzeyi değişkenlerine göre farklılık göstermekte midir?
5. Üniversite öğrencilerinin dijital vatandaşlık düzeyleri;
    - Cinsiyet,
    - Öğrenim görmekte olduğu eğitim kademesi,
    - Sınıf,
    - Günlük ortalama internet kullanma süresi,

- Teknolojik cihaz sahipliği,
- Ailenin aylık ortalama gelir düzeyi değişkenlerine göre farklılık göstermekte midir?

6. Dijital vatandaşlık farkındalığının ve bilgi düzeyinin artırılmasıyla ilgili olarak, öğrencilerin üniversite yönetiminden beklentileri nelerdir?
7. Dijital veri güvenliği konusunda farkındalığın ve bilgi düzeyinin artırılmasıyla ilgili olarak, öğrencilerin üniversite yönetiminden beklentileri nelerdir?

Tezin problemi doğrultusunda ilgili alan yazında yapılmış çalışmalar incelendiğinde; dijital veri güvenliği farkındalığı üzerine kısıtlı çalışmanın olduğu görüldüğünden, alan yazındaki boşluğu dolduracağı umulmaktadır. Toplumda iyi eğitilmiş ve dikkatli bireyler olası güvenlik ihlallerini engelleyebilir. Bu bağlamda çalışmadan elde edilecek sonuçların bireylerin dijital veri güvenliği hakkında bilinçlendirilmesi ve farkındalık yaratılması bakımından bireylerin en iyi şekilde geleceğe hazırlanması, dijital veri güvenliği farkındalığı oluşturmak bakımından gereken düzenlemelerin zamanında yapılmasının topluma katkı sağlayacağı düşünülmektedir. Bunun yanı sıra, böyle bir çalışmanın şimdiye kadar üniversite bazlı yapılmamış olması nedeniyle alan yazındaki boşluğu dolduracağı, aynı zamanda gelecekte bu alanda araştırma yapacak olan akademisyenlere de yol gösterici olacağı düşünülmektedir.

1.3. Sayıltılar

Araştırmaya katılan öğrencilerin ölçme araçlarına doğru, samimi ve içten yanıtlar verdikleri varsayılmıştır.

Araştırma kapsamında kullanılan ölçme araçlarının katılımcıların dijital vatandaşlık ve veri güvenliği farkındalığı düzeylerini doğru ölçtüğü varsayılmıştır.

1.4. Sınırlılıklar

Araştırma;

- 2021-2022 akademik yılı,
- Trakya Üniversitesi öğrencileri,
- Demografik Bilgiler, Dijital Vatandaşlık Ölçeği ve Dijital Veri Güvenliği Farkındalığı Ölçeği ile elde edilen verilerle sınırlandırılmıştır.

-

BÖLÜM 2

KAVRAMSAL ÇERÇEVE VE İLGİLİ ARAŞTIRMALAR

2.1. Dijital Vatandaşlık

Dijital vatandaşlık kavramı ilk olarak Mike Ribble ve Gerald Bailey (2007) tarafından ortaya atılmıştır (Sarı ve Taşer, 2018). Alan yazında dijital vatandaşlık kavramı hakkında çeşitli tanımlamalar yapıldığı görülmektedir. Çubukçu ve Bayzan'ın (2013) yaptığı tanımda dijital vatandaş, teknoloji ve teknolojik araçları doğru kullanabilen, istediği bilgilere kolaylıkla ulaşabilen, sahip olduğu güvenlik ve sorumluluk bilinci ile dijital ortamlarda bilinçli davranışlar sergileyen, etik kuralara göre hareket eden bireylerdir. Bir başka tanımlamada dijital vatandaş; dijital ortamlarda başkaları ile iletişimde etki kurallar çerçevesinde hareket eden, dijital ortamlardaki tehlikelerin bilincinde olup, yaşanabilecek tehlikelere karşı önlem almasını bilen kişidir (Aydın, 2015).

Dijital vatandaşlık kavramı vatandaşlığın geçmişten günümüze gelen bir biçimi olarak görülmektedir. Bilgi edinmek amacıyla doğru şekilde teknoloji ile kitle iletişim araçlarını kullanan kişiler ise dijital vatandaş olarak nitelendirilmektedir (Şimşek ve Şimşek, 2013). Eğitim kurumlarında vatandaşlık eğitimleri verildiği gibi dijital vatandaşlık eğitimlerinin de verilmesinin gerekli olduğu belirtilmektedir. Çünkü teknolojinin hem eğitim ortamlarında hem de dış ortamlarda olumsuz kullanımı her geçen zaman artış göstermektedir (Kaya ve Kaya, 2014). Fingal (2017) tarafından iyi dijital vatandaşın özellikleri aşağıdaki gibi belirtmektedir:

- Eşit dijital haklara sahip olma, herkese erişimin sağlanmasını savunmak,
- Perspektiflerin tümünü anlamaya çalışmak,

- Fikri mülkiyet haklarına, diğer bireylerin çevrimiçi haklarına, dijital mahremiyete saygı göstermek,
- Dijital ortamlardaki kaynaklara eleştirel yaklaşma, doğru olmayan reklamları ve haberleri, güvenilir olmayan kaynakları paylaşmamak,
- Dijital ortamlarda diğer kişilere empati ile yaklaşarak iletişim kurmak,
- Dijital araçları duygusal, zihinsel ve fiziksel sağlığa dikkat ederek kullanmak,
- Sosyal nedenleri teknolojiden yararlanarak savunmak ve ilerletmek,
- Dijital kimliği proaktif yönetmek, dijital dünyanın kalıcı olduğunu anlamak,
- Dijital araçlardan yararlanarak başkaları ile iş birliği yapmak.

Bu çalışmada, bireylerin iyi birer dijital vatandaş olabilmeleri için Fingal (2017)'in belirttiği özelliklere sahip olmaları gerektiği düşünülmektedir.

Bilgi ve iletişim teknolojilerinde yaşanan hızlı gelişim ve dönüşüm dijital teknolojilerin farklı alanlarda kullanımını yaygınlaştırmaktadır. Buna paralel olarak insanlar da mekân fark etmeksizin bilgiye ulaşabilmekte, internetin haberleşme ve iletişim konularında sınırları kaldırması ile bireyler dünyanın her yerinden farklı ülke vatandaşları ile iletişim kurabilmektedirler. Bireyin vatandaş olarak dijital ortama girmesi sonucunda ise dijital vatandaşlık kavramı ortaya çıkmıştır (Karaduman ve Öncül, 2019).

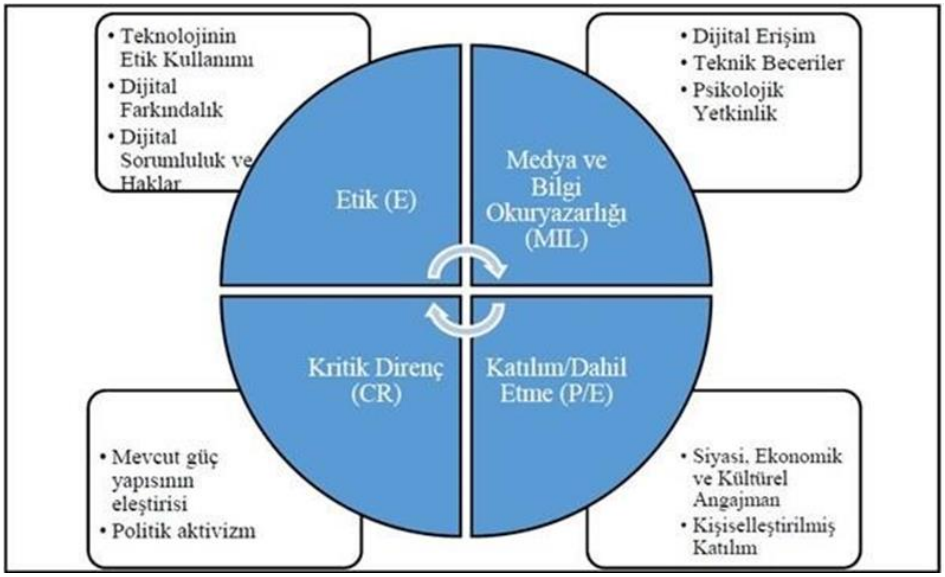
Dijital vatandaş yerel, ulusal ve küresel nitelikteki dijital ortamlara etkin, aktif ve sorumlu şekilde katılmayı başaran kişi olarak ifade edilmektedir (Telli, 2020). Dijital vatandaşlık kavramı içeriğinde katılım, paylaşma, üretme, araştırma, sosyalleşme, tüketme, eğitim- öğretim, iletişim gibi pek çok faaliyeti barındırmaktadır. Dijital vatandaş, dijital ortamda eleştirel düşünen, bilgi alırken ya da paylaşırken doğru davranış sergileyen, etik boyutları tartışan birey olarak ifade edilmektedir (Mercimek, Yaman, Kelek ve Odabaşı, 2016). Searson, Hancock, Soheil ve Shepherd (2015) tarafından ise dijital vatandaşlık, özellikle bireylerin işbirlikli ortamlarda mobil araçlar, bilgisayar, tablet, cep telefonu gibi dijital araçları kullanırken davranışlarının bir özelliği şeklinde tanımlanmaktadır.

Teknolojide yaşanan hızlı dönüşüm ve gelişim günümüz öğrencilerini de etkilemiş ve değiştirmiştir. Günümüzde öğrenciler cep telefonları, bilgisayarlar, video oyunları ile dijital dünyadaki diğer araçlarla çevrelenmiştir. Akıllı telefonlar, bilgisayar oyunları, anlık mesajlaşma bir anlamda yaşamlarının vazgeçilmez parçası haline

gelmiştir. Bireylerin yetişme tarzları sonucunda bilgiyi işleme ve düşünme şekilleri kendilerinden önceki kuşaklardan daha farklıdır. Bundan dolayı "Dijital Yerli" olarak nitelendirilirler. Dijital yerlilerin bilgi ile ilişkileri, arkadaşlık ilişkileri, bilgiyi ele alma biçimleri aileleri ile kendilerinden önceki kuşaktan daha farklıdır. Yaşamlarını idame ettirmek için gereken bilgilerin tümünü dijital ortamdan alabileceklerine güven duyarlar (Karaduman ve Öztürk, 2014). Dijital yerlilerin farklılığı, farklı şekillerde tanımlanması, teknolojideki hızlı ilerlemeye bağlı olarak daha fazla olanağa, daha fazla erişime sahip olacakları, dijital ortamlardaki hareketlerinin yeniliklere neden olacağı şeklinde yorumlanmaktadır (Teo, Kabakçı Yurdakul ve Ursavaş, 2014).

2.1.1. Dijital Vatandaşlığın Boyutları

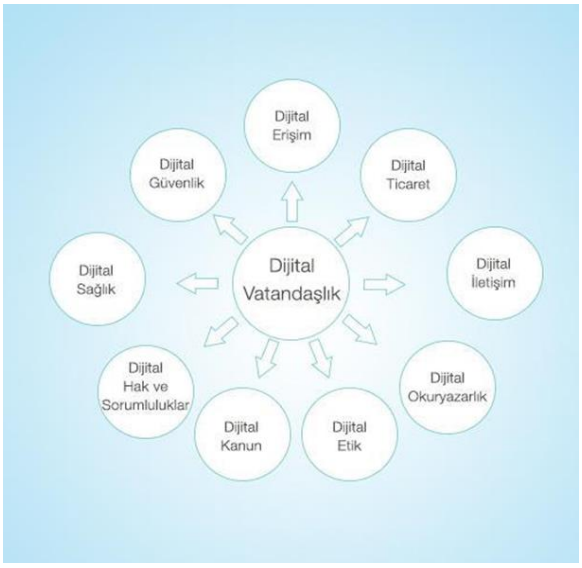
Alan yazında dijital vatandaşlığın boyutları ile ilgili olarak farklı sınıflandırmaların yapılmış olduğu görülmektedir. Bunlardan biri Oyedemi (2012) tarafından yapılan sınıflandırmadır. Dijital vatandaşlık boyutları bu sınıflandırmada; Vatandaşlık ve insan hakları, iletişim teknolojilerine erişim ve uygulayabilme becerisi, teknolojilerin düzenli kullanılabilmesi, bu bileşenlerin uygulanabilirliğini mümkün kılan politika olarak beş boyut ele alınmıştır. Choi (2016) tarafından yapılan sınıflandırmada ise dijital vatandaşlık 4 boyut halinde ele alınmıştır. Bunlar Şekil 2.1'de yer aldığı gibi Medya ve Bilgi Okuryazarlığı, Dijital Etik, Katılım, Kritik Direnç olarak tanımlanmaktadır.



Şekil 2.1. Dijital Vatandaşlığın 4 Boyutu (Choi, 2016)

Choi (2016) tarafından yapılan sınıflandırmada dijital vatandaşlığın dijital etik boyutu; dijital ortamda sorumlu ve etik davranışlarda bulunmayı, dijital teknolojilerden kaynaklı sosyal, kültürel ve politik sorunların farkındalığını, kişisel bilgilerin korunmasını, siber zorbalığın önlenmesini içeren dijital hakları ve sorumlulukları içermektedir (Ribble, 2004; Ohler, 2012; Winn, 2012). Medya ve bilgi okuryazarlığı boyutu; bilgiye ihtiyacı anlama, bilgiye erişimi, bilgiyi değerlendirmeyi, bilgiyi sentezlemeyi, çevrimiçi iletişimin bilinmesini içermektedir (Moeller, Joseph, Lau ve Carbo, 2011). Katılım boyutu; sosyo-ekonomik, kültürel ve politik katılım gibi farklı çevrimiçi etkileşim türlerini içermektedir. Kritik direnç boyutu ise; daha doğrusal, yenilikçi, hiyerarşik, yaratıcı olmayan katılım biçimlerini içermekte, potansiyel olarak derin dijital etkileşimi içermektedir (Choi, 2016; Yalçınkaya, Cibaroğlu, 2019).

Alan yazında dijital vatandaşlığa ilişkin farklı sınıflandırmalar ve açıklamalar yapılsa da yaygın olarak kullanılan sınıflandırmanın Ribble (2004, 2011) tarafından yapılan sınıflandırma olduğu görülmektedir. Bu sınıflandırmada Şekil 2.2'de yer aldığı üzere dijital vatandaşlık; dijital erişim, dijital okuryazarlık, dijital iletişim, dijital haklar ve sorumluluklar, dijital hukuk, dijital etik, dijital güvenlik ve dijital sağlık olmak üzere dokuz boyut halinde temellendirilmiştir. Dijital vatandaşlığın dokuz boyutu bilgi okuryazarlığı düzeyi yüksek yeni vatandaş tipini yetiştirmeyi amaçlamaktadır. Dijital vatandaşlık boyutları günümüzde bireylerin sahip olmaları gereken özellikler arasında olduğu kabul edilebilir.



Şekil 2.2. Dijital Vatandaşlığın 9 Boyutu (Yalçınkaya ve Cibaroğlu, 2019)

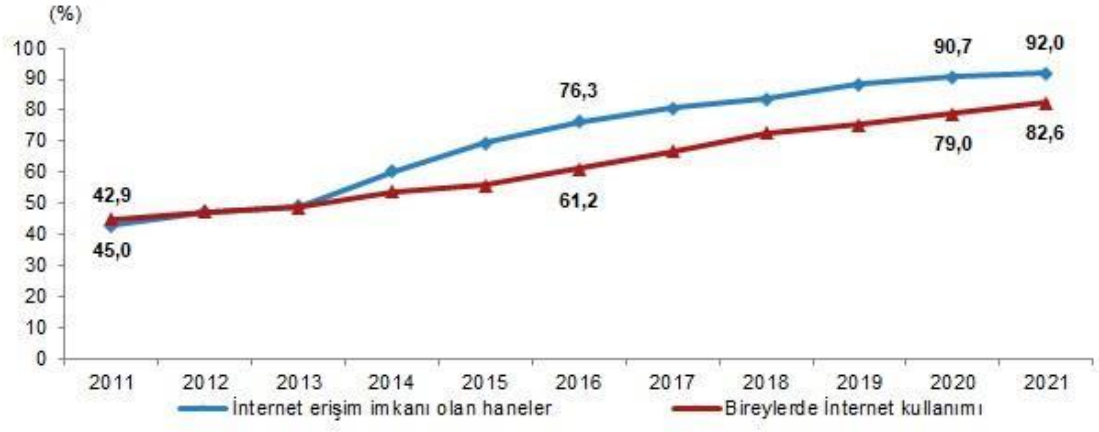
Dijital vatandaşlığın dokuz boyutu aşağıdaki gibi açıklanabilir:

a. Dijital Okuryazarlık: Günümüzde teknolojinin her geçen gün kullanım alanlarının yaygınlaşması ile birlikte bireyler için geçmişte yeterli olan okuryazarlık türleri de farklılaşmaya başlamış, yeni okuryazarlık türlerinin ortaya çıkması ile yeni yetkinliklere ihtiyaç duyulduğu ifade edilmiştir (Şimşek ve Şimşek, 2013). Dijital okuryazarlık genel olarak teknoloji kullanımı ve dijital ortamlar üzerine öğrenme-öğretimin gerçekleştirilme süreci olarak tanımlanmaktadır (Ribble, 2011). Diğer bir ifade ile bireylerin interneti ve teknolojik cihazları bilgiye ulaşma ya da bilgiyi toplumdaki diğer üyeler ile paylaşma amacıyla kullanmasıdır. Bireylerin kendi başlarına istedikleri bilgiye ulaşması veya bilgiyi diğerlerine öğretmesi mümkün oluyorsa, bireyler dijital okuryazar olarak nitelendirilebilmektedir. Bununla birlikte güvenilir kaynak belirleme becerisi, program kullanma becerisi veya araştırma yapma becerisi dijital okuryazarlık gereklilikleri arasındadır (Suson, 2019). Günümüzde dijital okuryazarlık bilinen anlamıyla okuryazarlıktan daha önemli konuma gelmiş olup, dijital vatandaşlık eğitiminde en önemli öğeler arasında yerini almış olduğu görülmektedir (Çubukçu ve Bayzan, 2013).

b. Dijital Erişim: Dijital vatandaşlığın bu boyutu dünyada herkesin interneti ve teknolojik cihazları kullanabileceği altyapı ve olanaklara sahip olabilmesini ifade etmektedir. Bu olanaklar ırk, din, dil, zihinsel ve fiziksel ayrım olmaksızın herkese aynı kalitede ve hızda olan teknoloji olanağının sunulmasını belirtmektedir (Sakallı, 2015). Dijital erişim bir başka tanımda toplumda herkesin dijital ortamlara tam olarak katılımı olarak ifade edilmektedir (Ribble, 2011). Alberta Education (2012) tarafından da dijital erişim tamamen dijital ortamlara katılabilme şeklinde tanımlanmaktadır. Orhon (2019) tarafından ise teknoloji kanallarının aktif kullanımı dijital erişim olarak ifade edilmiştir.

Dijital vatandaşlık açısından internete ve dijital platformlara erişim kolaylığının önem arz etmesi, bir anlamda toplum içinde önemini göstermektedir (Mossberger, Tolbert ve Hamilton, 2012). Her bireyin dijital toplumlarda olsalar da benzer olanaklara sahip olamamaları ise önemli bir sorun olarak kabul edilebilir. Altyapı problemi, özel gereksinimler, coğrafi konum gibi nedenlerle bireylerin internete ve dijital platformlara

erişimi aynı toplumda yer alsalar dahi bireylere göre farklılıklar gösterebilmektedir (Ribble, 2011). Bu doğrultuda Türkiye'de hanelerin ve bireylerin erişimi Şekil 2.3'te yer aldığı üzere Türkiye İstatistik Kurumu (TÜİK) verileri üzerinden incelenebilir.



Şekil 2.3. İnternet Erişimi Olan Hanelerde ve Bireylerde İnternet Kullanım Oranı 2011-2021 (TÜİK, 2021)

TÜİK (2021) verilerine göre; 2021 yılı internet kullanım oranları 16-74 yaş aralığındaki bireylerde %82,6 olarak gerçekleşmiştir. 2020 yılında bu oran %79,0 olmuştur. Hanelerin ise 2020 yılında %90,7 olan internete erişim olanağı, 2021 yılında %92,0'ye yükselmiştir. Cinsiyete göre internet kullanım oranı ise erkeklerde %87,7 iken, kadınlarda %77,5 olarak gerçekleşmiştir.

Bireylerin internet kullanım sıklığına ilişkin veriler ise Çizelge 2.1'de görülmektedir.

Çizelge 2.1. Bireylerin İnternet Kullanım Sıklığı 2020-2021 (%) (TÜİK, 2021)

İnternet Kullanım Sıklığı	**Kadın**		**Erkek**		**Toplam**	
	2020	2021	2020	2021	2020	2021
Hemen her gün	65,3	71.4	76,4	81,6	70,8	76,5
Haftada en az 1 defa	5,6	4,0	5,7	4,0	5,6	4,4
Haftada 1 defadan az	1.2	0,9	1.2	0,8	1,2	0,9

TÜİK (2021) verilerine göre; interneti düzenli kullanan bireylerin oranı 2020 yılında %70,8 iken 2021 yılında %80,5 olmuştur. 12021 yılının ilk üç ayında 16-74 yaş aralığındaki bireylerin %80,5'i interneti hemen her gün ya da haftada en az 1 gün düzenli olarak kullanmıştır. Bu verilerden bilişim teknolojilerinde yaşanan gelişmelerle birlikte dijital ortamlara erişimin kolaylaştığı, bundan dolayı insanların dijital erişim oranının her yıl arttığı belirtilebilir.

Dijital erişim kavramına ilişkin sorunlar aşağıdaki başlıklar halinde ele alınabilir (Telli, 2020):

- Maddi erişim: Teknolojiye yönelik altyapıya veya gereken donanıma sahip olmamak,
- Zihinsel erişim: Bilgisayar korkusu, yeni teknolojilerin ilgi çekmemesi gibi nedenlerden dolayı dijital deneyim yaşayamamak.
- Kullanım erişimi: Dijital ortamda önem arz eden kullanım fırsatlarını kaçırmak.
- Deneyim erişimi: Eğitimden kaynaklı destek eksikliği nedeniyle deneyim eksikliği yaşamak.

Dijital erişim ile ilgili bu sorunlar arasından birine veya birden fazlasına sahip olmak dijital bölünme veya dijital uçurum olarak ifade edilmektedir. Dijital bölünme; yeni dijital biçimlerine erişimi bulunanlar ile bulunmayanlar arasındaki boşluk olarak tanımlanmaktadır. Aynı zamanda dijital teknolojileri kullanma becerisi, bilgisi ve yetenekleri bulunanlar ile bulunmayanlar arasındaki tutarsızlık da dijital bölünme olarak ifade edilmektedir (Telli, 2020). Günümüz eğitim sisteminde de çeşitli açılardan bireyler arasında dijital bölünme olduğu görülmektedir (Kurt, Günüç ve Ersoy, 2013). Bundan dolayı genç yaşlarda bireylere dijital vatandaşlık bilincinin öğretilmesi ve bu bilincin arttırılması gerekliliği bulunmaktadır (Som Vural ve Kurt, 2018).

c. Dijital İletişim: Teknolojik gelişmelere paralel iletişimin dijitale taşınması ile birlikte dijital iletişim kavramı doğmuştur. Ribble (2011) tarafından dijital iletişim kavramı elektronik bilgi alışverişi olarak, Uluslararası Eğitimde Teknoloji Topluluğu (ISTE) (2020) ise farklı dijital kanallardan iletişim kurma esnasında doğru kararların verilebilmesi olarak tanımlamaktadır. Dijital vatandaşlık boyutlarından biri olan dijital iletişim; bireyin dijital vatandaş olarak nitelendirilebilmesi için dijital iletişim araçları ile iletişime geçebilmesini ifade etmektedir (Çebi, 2020).

Bireylerin dijital iletişim kurabilmelerinin temeli dijital platformları etkin ve doğru kullanmalarını sağlayacak düzeyde bilgi ve beceriye sahip olmalarına dayanmaktadır. Diğer bir ifade ile dijital vatandaş olmak için dijital ortamda bilgi aktarımını yapabilecek düzeyde beceri sahibi olmak gerekir. Bireylerin dijital iletişim araçlarına ilişkin sahip olmaları gereken beceri, iletişim araçlarının nasıl kullanılacağını ve kişisel verilerin korunması amacıyla hangi güvenlik ayarlarının yapılacağını bilmeleridir (Mısırlı, 2020).

Bireyleri dijital iletişim açısından engelleyen bazı etkenler bulunmaktadır. Bu etkenler kimlik, duygusal, fiziksel, erişim, semantik, güvenlik ve dikkat olarak sınıflandırılmaktadır. Bunların arasında bireyleri en fazla etkileyen fiziksel etkenler, çevrimiçi ve çevrimdışı iletişimde çeşitli zorluklar içerir. Dijital iletişimi engelleyen fiziksel etkenler arasında yer, ortam ve zaman gibi çevresel koşullar yer almaktadır (Girardin, 2020).

Dijital iletişimin bireylere sağladığı bazı kolaylıklar bulunmaktadır (Yılmaz, 2019):

- Anlık haberleşme olanağı,
- Veri paylaşımı yapabilme olanağı,
- Görsel iletişim sağlama,
- Bağlantı gönderebilme olanağı.

Günümüzde dijital iletişim amacıyla kullanımı her geçen zaman yaygınlaşan teknolojik araçlar olarak mobil cihazlar, akıllı televizyonlar, akıllı saatler, masaüstü ve dizüstü bilgisayarlar gösterilebilir (Yılmaz, 2019).

d. Dijital Hukuk: Dijital teknolojiler internette çeşitli materyallerin bulunmasını, indirilmesini ve paylaşılmasını kolaylaştırmıştır. İnternetin en güçlü yönleri arasında yer alan bilgiyi kolay paylaşma seçeneği olsa da kullanıcılar hangisini uygun hangisinin uygun olmadığını, materyallerin yasa dışı olabileceği ihtimalini düşünmezler (Ribble, 2011). İnternetin hızla yaygınlaşması ile oluşan toplumsal yapıda bireylerin temel sorunları arasında neyin sahte olduğu neyin gerçek olduğu karmaşasıdır. Bunun yarattığı sorunların çözümünde ise dijital hukuk kavramı öne çıkmaktadır. Dijital hukuk kavramı dijital ortamlarda gerek duyulan yasal gereksinimler, etik kurallar ve kararlar ile ilişkili bir kavramdır (Ribble (2015).

Bilişim teknolojilerin kullanılması ile gerçekleştirilen suçlar siber suçlar veya bilişim suçları olarak tanımlanmaktadır. Çevrimiçi ortamdaki dolandırıcılık, verileri silme- yok etme, bilişim sistemlerini engelleme veya bozma, nitelikli dolandırıcılık, şantaj, taciz, özel hayatın gizliliğini ihlal, dijital kimlik hırsızlığı, dosya paylaşım siteleri aracılığıyla izin alınmadan indirilen dokümanlar ve belgeler, haberleşmenin gizliliği bilişim suçları kapsamında bulunmaktadır (Ribble ve Bailey, 2007). Dijital vatandaşların dijital ortamlarda da günlük hayatlarında olduğu gibi kanunlara uygun davranmaya özen göstermeleri gerektiği söylenebilir.

Ribble (2011) tarafından yürütülen çalışmada yasal ve yasadışı teknoloji kullanımına ilişkin olarak bireylerin yapmaları ve yapmamaları gereken davranışlar örneklerle bildirilmiştir. Bireylerin telif hakkı bulunan müzikleri dosya paylaşım siteleri veya sosyal ağlardan yasal olmayan yollardan indirmesi, güvenlik duvarlarını yıkacak yasal olmayan yazılım kullanmaları yasadışı teknoloji kullanımına örnek olarak gösterilmiştir. Bireylerin telif hakkı ile korunan materyalleri, nelerin ücretsiz indirilebileceğini kabullenmesi ve ücret ödemesi gibi örnekler ise yasal teknoloji kullanımına örnek olarak gösterilmiştir.

e. Dijital Ticaret: Mal ya da hizmetin satılması ve satın alınması ticaret olarak; ticaretin çevrimiçi ortamda yapılması ise dijital ticaret olarak tanımlanmaktadır (Karaduman, 2011). Dijital ticaret kavramı, bireylerin internet yardımıyla dijital ortamlarda bir şeyleri satın alması veya satabilmesi, bankacılık işlemlerini yapabilmesi, bunları güvenliklerini sağlayarak yapabilmesini ifade etmektedir (Çubukçu ve Bayzan, 2013).

Ribble (2011) tarafından yapılan çalışmada dijital ticarete ilişkin bazı riskler aşağıdaki gibi sıralanmıştır:

- Müzayede sitelerin aracılığıyla yapılan çevrimiçi ürün alım satımında oluşabilecek riskler,
- Açık arttırma siteleri, ticaret siteleri ve diğer siteler aracılığıyla yapılan çevrimiçi ürün alım satımında oluşabilecek riskler,
- Bireylerin kimliklerini ne şekilde koruyacaklarını bilmeden yaptıkları çevrimiçi ürün alım satımından kaynaklanan kimlik hırsızlığı riski,
- Dolandırıcılık ile karşı karşıya kalma riski,

- Çevrimiçi oyunlar için yapılan ürün/sanal anahtar alım satımında oluşabilecek riskler.

f. Dijital Hak ve Sorumluluklar: Toplumda yaşamı sürdürebilmek gibi dijital ortamlarda var olabilmek için hak ve sorumluluklar ile karşı karşıya kalınmaktadır (Alberta Education, 2012). Dijital ortamlar hem herkesin sınırsız olarak kendini ifade edebilme özgürlüğünün olduğu hem de diğer bireylerin kişisel haklarının ihlal edilmemesi gereken platformlardır. Örneğin; dijital ortamda bilgi araştırması yapılırken ilgili bilginin üzerindeki haklar ve haklara ilişkin çevrimiçi sorumlulukların bilinmesi gerekmektedir (Çubukçu ve Bayzan, 2013). Dijital toplum içerisinde yer almak, her bireyin belirli haklarının olduğunu, her bireye bu hakların eşit olarak sağlanmasını ifade etmektedir. Bu durum dijital vatandaşların da topluma karşı belirli sorumluluklarının olduğunu belirtmektedir (Ribble, 2011). Bireylerin bu hak ve sorumlulukların farkında olabilmesi için dijital etik kurallarına uygun olarak dijital ortamlarda faaliyetlerini nasıl gerçekleştireceklerini, olumsuz davranışları gerçekleştirmek amacıyla teknolojiyi kullanmamaları gerektiğini bilmeleri gerekmektedir (Karaduman ve Öncül, 2019). Bu nedenle bireylere eğitimler verilerek, dijital hak ve sorumluluklar kazandırılmalıdır. Vatandaşların bilinçli yetiştirilmesi her ülke için önemli olması yanında bireylerin dijital ortamlarda hak ve sorumluluklarını bilenler olması etik anlamda olduğu kadar yasalara uyma anlamında da kendinin farkında bireyler olmalarına ve toplum sorunlarının azaltılmasında rol oynamaktadır (Elçi, 2015).

Ribble (2011) yaptığı çalışmasında bireylerin uymaları gereken hak ve sorumluluklarının bazılarını aşağıdaki gibi sıralamaktadır:

- Teknolojiyi sorumlu şekilde kullanmak ve kabul edilebilir kullanım politikalarının takip edilmesi,
- İzin talep etmek, kaynak göstermek gibi çevrimiçi materyallerin etik olarak kullanılması,
- Tehditlerin, siber zorbalıkların ve uygunsuz olan diğer durumların yapılmaması,
- İnternetten elde edilen bilgilerin veya materyallerin kaynak belirtilerek kullanılması.

g. Dijital Etik: Bireylerin interneti ve teknolojik cihazları kullanırken etik kurallara uygun saygılı davranışlar sergilemesi, başkalarını rahatsız edici olmayan

sorumluluk sahibi olmaları dijital etik olarak ifade edilmektedir. Dijital etik, bazı araştırmacılar tarafında ise tam elektronik katılım şeklinde tanımlanmaktadır (Elçi, 2015). Aynı zamanda bireylerin yazılı olmayan dijital etik normlarını, kurallarını veya değişimleri gözlemleyebilmesi şeklinde de tanımlanmaktadır (Hollandsworth vd., 2011). Dijital vatandaşlığın dijital etik boyutu; teknolojik cihazların ne zaman ve nasıl kullanılacağının bilincinde olunması ve başkalarına saygı duyulması anlamına gelmektedir (Çubukcu ve Bayzan, 2013). Bir başka tanımda dijital etik; dijital ortamlarda diğer kişilerin hoşlanmayacağı davranışlardan kaçınma şeklinde ifade edilmiştir (Çakmak, 2016). Ocak (2013) tarafından dijital etiğin ihlal edildiği bazı davranışlar aşağıdaki gibi sıralanmıştır:

- İzinsiz olarak kişisel verilerin elde edilmesi
- Yanlış bilgi yayılması
- Telif hakkı ihlallerinde bulunulması
- Özel yaşam ihlalleri
- İntihal
- Siber zorbalık davranışları sergilenmesi

Bireylerin iyi dijital vatandaş olmalarında dijital etik boyutunun önemli olduğu söylenebilir. Dijital etik boyutunun, bireylerin kaçınması gereken davranışlar yanında kendi iradesi ile yapması gereken davranışları da kapsadığı belirtilebilir.

Dijital araçların kullanımında başkalarına saygılı olma sorumluluğu her dijital vatandaşın sahip olması gereken özellikler arasında yer almaktadır. Bireyler çevresindekileri izleyerek bir teknolojinin nasıl kullanıldığını ve nasıl kullanılmayacağını öğrenirler. Dijital teknolojilerin yaygınlaşması bireyler için de yeni öğrenme alanı oluşturmuştur. Bireylerin bir kısmı hızlı bir şekilde öğrenirken, bir kısmı dijital teknolojileri kullanırken hangi kurallara uyulması gerektiğini genelde anlamazlar (Ribble, 2011).

Dijital bir toplumda yer almak bireylere bazı sorumluluklar yükler. Öncelikle teknoloji kullanımının diğer bireyleri nasıl etkilediği göz önüne alınmalıdır. İyi dijital vatandaşlar diğerlerine saygılı olur, teknolojiyi etkili şekilde nasıl kullanacaklarını öğrenirler. Dijital görgü kuralları ise aşağıdaki şekilde sıralanabilmektedir (Ribble, 2011):

- Teknolojiyi kullanılırken başkalarına olan olumsuz etkilerin en aza indirilmesi,
- Dijital ortamlarda başkalarına saygılı olmak,
- Teknolojiyi bağlamsal olarak uygun olduğunda kullanmak,
- Kışkırtıcı olmamak, siber zorbalık içeren davranışlarda bulunmamak,
- Hangi bilgilerin paylaşılabildiğini, paylaşımın ne zaman uygun olduğunun bilincinde olmak.

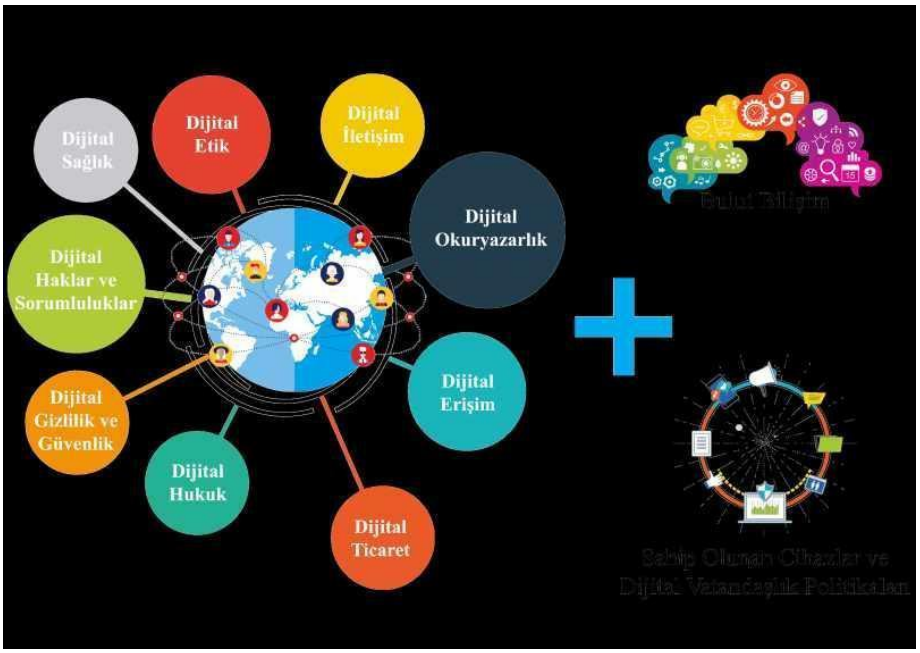
h. Dijital Sağlık: Dijital vatandaşlık boyutlarından olan dijital sağlık, dijital ortamda ruhsal ve fiziksel olarak sağlıklı olmayı ifade etmektedir. Bireyler süreç içerisinde kendi sağlıklarını koruma amacıyla önlem almalı, gerektiği takdirde interneti ve dijital araçları kullanmamaları önem arz etmektedir (Elçi ve Sarı, 2016). Dijital teknolojileri ile birlikte yeni sağlık problemlerinin ortaya çıktığı belirtilebilir. Sağlık sorunlarının önlenmesi için bireylere uygun internet ve bilgisayar kullanımının öğretilmesi gerekir. Bireylerin uygun ergonomik yerlerden dijital ortamlara bağlanması, teknolojiye ne kadar zaman ayrılmasının gerektiğinin farkında olması gerekmektedir. Bunun sağlanamaması ise dijital vatandaşlığın temelini oluşturan çevrimiçi kaynakların doğru olarak kullanımını ve doğru bilgiye erişimi etkileyerek, bireylere maddi- manevi zarar vererek dijital sağlığın gündem olmasına, yetkili birimlerin işlevlerini yerine getirmelerini zorlaştırmaktadır (Aldemir ve Avşar, 2020, s.159).

ı. Dijital Güvenlik: Teknoloji kullanımının giderek artması ile birlikte insanların işlemlerinin pek çoğunu internet üzerinden dijital platformlarda yapmalarına uygun zemin hazırladığı söylenebilir. Dijital ortamlardaki bilgi paylaşımları, alışverişler, sosyal ilişkiler, mali konular sadece güvenli internet ortamında yapılabilir. Bu doğrultuda dijital güvenlik; dijital vatandaşın internette kendisinin, donanım, ağ ve yazılım gibi araçların güvenliklerini sağlayabilmesi şeklinde tanımlanabilir. Diğer bir anlatımla dijital güvenlik, internet ve dijital teknolojilerle olan ilişkilerde dijital kimliğin ve kişisel güvenliğin korunması amacıyla gerçek hayattaki gibi önlemlerin alınması olarak ifade edilebilir. Örneğin; bir kişi evinin kapısını açık bıraktığında değerli eşyaların çalınma riski taşır. Benzer şekilde bir kişi internet kafede giriş yaptığı bir web sitesinden çıkış yapmaz açık bırakırsa aynı tehlike ile karşılaşabilmektedir (Filiz, 2020).

Bilgi teknolojilerinin yoğun kullanıldığı günümüzde dijital vatandaşların kendi güvenlik önlemlerini alma zorunlulukları bulunmaktadır. İnternet ve dijital ortamlarda

güvenliği olumsuz etkileyen siber saldırılar bireysel olduğu kadar toplumsal bir tehdit unsuru olmaktadır (Çubukcu ve Bayzan, 2013). Dijital güvenlik bakımından en yaygın görülen saldırı ve tehditler ise; Truva atları, solucanlar, virüsler, hacker saldırıları, olta ve tuş kaydediciler, paylaşıma açılan zararlı olan dosyalar, transfer edilecek olan bilginin değiştirilmesi, sahte anti-virüs yazılımları, üçüncü kişilerin gizli bilgileri öğrenmesi şeklinde sıralanabilmektedir (Çakır ve Kesler, 2012).

Alberta Education (2012) tarafından dijital vatandaşlığın Ribble'un (2004, 2011) belirlemiş olduğu dokuz boyutuna ek olarak Şekil 2.4'te yer aldığı üzere bulut bilişim boyutu ile sahip olunan cihazlar ve dijital vatandaşlık boyutları eklenmiş ve dijital vatandaşlık boyutlarının 11 olması gerektiği ifade edilmiştir.



Şekil 2.4. Dijital Vatandaşlığın 11 Boyutu (Alberta Education, 2012)

Dijital vatandaşlığın dokuz boyutuna eklenen bulut bilişim boyutu ile sahip olunan cihazlar ve dijital vatandaşlık boyutlarına bakıldığında;

Bulut Bilişim: Dijital vatandaşlığın bu boyutu verilerin toplanması, yönetilmesi ve işlenmesi için internette uzak sunucuların kullanımını ifade etmektedir. Bulut bilişim boyutunun temel özelliği ise kullanıcı için şeffaf olma eğilimini göstermesidir. Bunun yanı sıra herhangi bir ayrıntı düzeyinde anlaşılması net değildir. Diğer bir anlatımla bulut bilişim, kullanıcılar açısından kolay bir hizmet olmaktadır. Bununla birlikte kullanıcılar

fiziksel olarak bulut bilişim sunucularının nerede olduğunu bilmemektedir. Bundan dolayı bulut bilişim ayrıntılarına fazla hâkim değildirler.

Sahip Olunan Cihazlar ve Dijital Vatandaşlık Politikaları: Dijital vatandaşlığın bu boyutu öğrenciler açısından ele alınmakta, öğrencilerin okula kendi teknolojik cihazları ile gittikleri kabul edilmektedir. Öğrenciler ile öğrencilerin etkili öğrenmeleri amacıyla fırsatlar sunan okul yöneticileri modeli uygun görmektedir. Öğrenimin okul sınırları ile içerisinde kalmadığı, bu teknolojik cihazlarla da öğrencilerin öğrenime devam ettikleri düşünülmektedir (Alberta Education, 2012).

2.1.2. Dijital Vatandaşlık Farkındalığı Konusunda Türkiye'de Yapılan Çalışmalar

Hayat Eve Sığar Uygulaması (HES): Şekil 2.5'te yer alan bu mobil uygulama pandemi sürecinde teknolojinin olanaklarından yararlanılarak, süreci sağlık bilişim sistemleri ile takip ve kontrol eden Türkiye Cumhuriyeti Sağlık Bakanlığı tarafından hizmete sunulmuştur.



Şekil 2.5. Hayat Eve Sığar Uygulaması (HES Uygulaması, 2019)

HES uygulaması ile vatandaşlar gitmek istedikleri veya yaşadıkları bölgede Covid-19 yoğunluğunu veya riskini harita üzerinden takip edebilmektedir. Uygulamada listeye eklenen arkadaşların ya da aile üyelerinin riskli yerlerden uzak kalmasını sağlamak için takip edilmesi mümkün olabilmektedir. Uygulamanın kullanım yerleri arasında resmi- özel kurumlar ile seyahatler de bulunmaktadır. Pandemide seyahatler sırasında zorunlu tutulan HES kodu uygulama aracılığıyla temin edilebilmektedir. Resmi-özel kurumlarda ise riski azaltmak için girişte HES uygulaması ile bireyin Covid-19 riski görülebilmektedir (HES Uygulaması, 2019).

E-Nabız: Bu dijital vatandaşlık uygulaması vatandaşların ve sağlık profesyonellerinin sağlık kuruluşlarından alınan sağlık verilerine mobil cihazlar ve internet üzerinden erişmelerini sağlamaktadır. Uygulamada sağlık bilgilerinin tümü yönetilebilmekte, tıbbi özgeçmişe ulaşılabilmektedir. E-Nabız uygulamasından yetki verildiği takdirde hekimler tarafından bireyin sağlık kayıtları değerlendirilebilir. Bu şekilde tanı ve tedavi süreci daha hızlı ve kaliteli yürütülebilir. Aynı zamanda kapsamlı sağlık bilişim alt yapısına sahip olan uygulama üzerinden çeşitli sağlık hizmetlerine kolaylıkla erişilebilir (E-Nabız, 2022).

Merkezi Hekim Randevu Sistemi (MHRS): Türkiye'de sağlık hizmetlerine verimli ve etkin şekilde ulaşılabilmesi amacıyla T.C. Sağlık Bakanlığı tarafından "Sağlıkta Dönüşüm Projesi" yürürlüğü konmuştur. Merkezi Hekim Randevu Sistemi (MHRS) ise bu programın önemli uygulamaları arasında yer almaktadır. MHRS uygulaması, teknolojik olanakların etkin kamu hizmetine dönüştürülmesini sağlayarak, vatandaşların hızlı ve kolay şekilde sağlık hizmetlerine ulaşmasını sağlamaktadır. Uygulama sayesinde hızlı ve kolay randevu alınabilmekte, aynı zamanda E-Nabız sistemi, kişisel sağlık sistemi, sesli hatırlatma sistemi ile birlikte hareket ederek çeşitli hizmetler sunmaktadır (MHRS, 2022).

DQ World (Türkçe): DQ Enstitüsü (DQI), sosyal yardım ve politikalar, dijital zekâ eğitimi için küresel düzeyde standartlar belirlemeyi amaçlayan uluslararası bir kuruluştur (DQI, 2022). Millî Eğitim Bakanlığı, DQI ve Türkcell ortaklığı ile "DQ World" Şekil 2.6'da görüldüğü gibi Türkçe olarak sunulmuştur. Projede çocukların dijital vatandaşlık farkındalıklarının arttırılması, güçlü birer dijital vatandaş yetiştirilmeleri amaçlanmaktadır (Bayer, 2018).



Şekil 2.6. DQ World (Türkçe) (Bayer, 2018; DQ World, 2022)

DQ World Türkçe 8-12 yaş aralığındaki çocuklar için hazırlanmış eğitsel oyun içerikleriyle dijital dünyaya gerektiği gibi hazırlanması amacıyla yapılmıştır. Şekil 2.7'de görülen çocuklara 8 temel DQ vatandaşlık becerisinin kazandırılması amaçlanmaktadır. DQ üç seviye halinde sekiz bilgi, alan, tutum, beceri ve değerlerden meydana gelen 24 yetkinliği içermektedir. DQ, kişinin hayatının tüm alanlarında dijital uygulamaların toplumsal ve bireysel refahın sağlanması için yönlendirmeyi amaçlamaktadır (Kritof, Zlaton ve Luka, 2018).



Şekil 2.7. Çocukların İhtiyacı Olan 8 Temel DQ Vatandaşlık Becerisi (DQ World, 2022)

DQ temel sekiz vatandaşlık becerisi ise dijital vatandaşlık kimliği, siber zorbalık yönetimi, gizlilik yöntemi, ekran süresi yönetimi, eleştirel düşünme, dijital empati, dijital ayak izleri ve siber güvenlik yönetimi olarak sıralanmıştır (DQ World, 2022).

Keşf@ Bilinçli İnternet Hareketi Projesi: İstanbul İl Milli Eğitim Müdürlüğü ve Google İnternet Geliştirme Kurulu ortaklığı ile geliştirilen Şekil 2.8'de görülen proje öğrencilerin dijital vatandaşlık farkındalıklarının arttırılması amacını taşımaktadır. Projenin hayata geçirilmesi internete ilişkin temel kavramların bilinmesi, dijital platformlarda bilgiye kolay ulaşma, etik davranışlarla dijital ortamların güvenli kullanımının sağlanması amacıyla öğrencilerin bilgilendirilmesi için gerçekleştirilmiştir.



Şekil 2.8. Bilinçli İnternet Hareketi Projesi (Bilinçli İnternet Hareketi Projesi, 2022)

Bilinçli İnternet Hareketi Projesi, sınıf içi etkinlikler ve eğitim materyallerinden meydana gelmektedir. Projenin kapsamında internet ile ilgili kavramlar, günlük internet kullanımı, dijital ortamlarda bilgiye hızlı ve etkin şekilde ulaşma, güvenilir dijital kaynakların kriterleri, dijital ortamlardaki tuzaklar ve siber saldırı önlemleri, güçlü parola üretme yöntemleri yer almaktadır (Bilinçli İnternet Hareketi Projesi, 2022)

İnternot Olmaya Var Mısın?: İnternet Güvenlik Koalisyonu ve Google tarafından çocukların çevrimiçi ortamlarda bilinçli ve güvenli şekilde hareket edebilmeleri amacıyla "İnternot Olmaya Var Mısın?" projesi tasarlanmıştır. Projede çocuklara, ebeveynler ve öğretmenlere ulaşılarak nesiller arası güçlü bir dijital diyalog sağlanması amaçlanmaktadır (Yapar, 2019). Google Türkiye ve Bilgi Teknolojileri ve İletişim Kurumu iş birliği ile Türkiye'de adını duyuran proje, dijital ortamlarda çocukların bilinçli olmalarını desteklemeyi planlamaktadır. Dijital ortamlarda güvende

olmak ve dijital vatandaşlık için tasarlanmış programın beş temel konusu aşağıdaki gibidir:

- Düşünerek paylaş
- Gerçek olduğundan emin ol
- Sırların sende kalsın
- İyi ol, özel ol
- Bir sorun olduğundan konuş.

Proje, bu temel konularda çocuklara çevrimiçi platformlardaki bilgilere yönelik eleştirel düşünceye sahip olmaları, olası sahtekarlıklar ve zorbalıklara karşı bilinçli davranmaları, doğru ve yanlış bilgileri ayırt etmeleri, paylaşımlarından kaynaklanabilecek sonuçlar hakkında bilgi sahibi olmaları, dijital ortamlardan dolayı oluşabilecek sorunlara ve tehditlere karşı hangi önlemlerin alınacağını bilmeleri, diğer kullanıcılara saygılı olmaları, zorluklarla karşılaştıklarında yardım istemeleri gibi davranışların bilinmesini planlamaktadır (Yapar, 2019).

Fırsatları Artırma ve Teknolojiyi İyileştirme Hareketi (Fatih Projesi): Bu proje eğitimde fırsat eşitliğinin sağlanması ve teknoloji kullanımının arttırılması amacıyla yapılmış olan kapsamlı bir projedir. Fatih projesi ile dijital vatandaşlıkta dijital erişim alt boyutu önem kazanmıştır. Dijitalleşen sınıflar ile eğitimde teknolojinin kullanımı mümkün olmuştur. Buna bağlı olarak öğretmenlerin yetkinliklerinin arttırılması zorunlu hale gelmiştir. Dijital dünyadaki en önemli sorunlar arasında öğrenciler ile öğretmenler arasındaki teknoloji yetkinliği uçurumudur. Fatih projesi ile öğretmenlere verilen hizmet içi eğitimlerle teknolojik yetkinlikleri arttırılmıştır. Çünkü öğretmenlerin dijital vatandaşlar olarak yetiştirecekleri öğrencilere örnek olmaları önem arz etmektedir (Fatih Projesi, 2019). Fatih projesinin erişilebilirlik, ölçülebilirlik, eşitlik, verimlilik ve kalite olmak üzere beş temel çerçevesi bulunmaktadır. Şekil 2.9'da yer alan projenin içeriğinde teknolojinin kaynaklara ulaşım kolaylığı sağlaması, öğrencilerin ders içeriklerini öğrenmelerini kolaylaştırması, eğitim teknolojilerinin kullanışlılığı, öğrenme ortamlarını zenginleştirmesi olumlu yönleri olarak görülmektedir (Demirer ve Dikmen, 2018).

Fatih projesi kapsamında eğitimde kullanılan etkileşimli tahtaların öğrenci ve öğretmenler tarafından benimsendiği, derslerde farklı amaçlar ve seviyelerde kullanıldığı,

ancak tablet kullanımının sınırlı olduğu belirtilmektedir (Pamuk, Çakır, Ergun, Yılmaz ve Ayas 2013).



Şekil 2.9. Fırsatları Artırma ve Teknolojiyi İyileştirme Hareketi (Fatih Projesi, 2019)

Fatih projesi hakkında öğretmenlerin bir kısmı faydalı olduğunu, bir kısmı ise projenin eğitimi herhangi bir katkı sağlamadığı görüşüne sahip olduğu bildirilmektedir (Altın ve Kalelioğlu, 2015)**.**

İzmir Üniversiteleri Platformu-Dijital Vatandaşlık Projesi: Bu proje İzmir Üniversiteleri Platformu tarafından 2019 yılında oluşturulmuş sosyal sorumluluk projesidir. Projenin amacı internetin bilinçli ve güvenli şekilde kullanılmasını, internet bağımlılığı, siber zorbalık gibi sorunlara dikkat çekmektir. Bunun yanı sıra bireylerin dijital vatandaşlık farkındalıklarının geliştirilmesini hedeflemektedir. Projenin başlangıcı Şekil 2.10'da görüldüğü üzere resmi internet sitesinde 17 Mayıs 2019 tarihinde başlatılan dijital vatandaşlık konulu karikatür yarışması ile gerçekleşmiştir (İzmir Üniversiteleri Platformu, 2019).



Şekil 2.10. Dijital Vatandaşlık Karikatür Yarışması (İzmir Üniversiteleri Platformu, 2019)

2.1.3. Dijital Vatandaşlık Farkındalığı Konusunda Dünyada Yapılan Çalışmalar

Avrupa Çevrimiçi Çocuklar Projesi (EuroKids Online): Bu çalışma çok uluslu bir araştırma ağı olup, Avrupalı çocukların dijital riskleri, fırsatları ve güvenliğine ilişkin bilgilerini geliştirmek amacıyla oluşturulmuştur. EuroKids Online, çocuklarda yeni medya kullanımını teşvik etmek ve koordine etmeyi amaçlamaktadır (EuKids Online, 2020).



Şekil 2.11. EuroKids Online (EuKids Online, 2020)

EuroKids Online projesi zamana yayılmış olan, devam eden bir projedir. Projede ilk çalışma 2006-2009 yılları arasında 21 ülkenin katılımı ile gerçekleşmiştir. Çalışmada Avrupalı çocukların internet kullanımına ilişkin kamuya açık veri tabanını oluşturmak

amacıyla araştırmalar belirlenmiştir. İkinci çalışma 2009-2011 yılları arasında 25 ülkenin katılımı ile gerçekleşmiştir. Çocuklar ve ebeveynlerin internet kullanımları, güvenlik ve risk deneyimlerine ilişkin orijinal veriler üretilmesi için yapılmıştır. Üçüncü çalışma 2011-2014 yıllarını kapsamış ve 33 ülke ağı ile gerçekleştirilmiştir. Güncellemeler yapılarak, çocuklar açısından sorunlu durumların uluslararası çalışması olmuştur. Dördüncü çalışma ise 2014-2018 yılları arasında 33 ülke tematik ağı ile gerçekleştirilmiştir. Bulgular kısa raporlarda yayınlanmıştır. Türkiye birinci EuroKids Online dışında diğerlerine katılmıştır (Aslan, 2016).

Sosyal Medya Okuryazarlığı (Social Media Literacy for Change-sml4change): Medya okuryazarlığı kavramı medyaya erişimi, medya ile etkileşimi ve medyanın eleştirel olarak anlaşılmasını sağlayan bilişsel, teknik, üretici, sivil, sosyal kapasiteleri içermektedir. Sosyal Medya Okuryazarlığı projesi ise Avrupa Komisyonu projesi olan Herkes İçin Medya Okuryazarlığı projesi ile birlikte finanse edilen öğretmenleri, okul liderlerini, gençlerle çalışanları destekleyen bir yıllık bir projedir (Sosyal Medya Okuryazarlığı, 2019).



Şekil 2.12. Social Media Literacy for Change (Sosyal Medya Okuryazarlığı, 2019)

Sosyal Medya Okuryazarlığı projesi kapsamında dijital vatandaşlık kursları da verilmektedir. Dijital vatandaşlık kursu dijital beceriler ve çevrimiçi güvenlik olmak üzere iki konuya odaklanmaktadır. Kursun öğrenme hedefleri aşağıdaki gibidir (Sosyal Medya Okuryazarlığı, 2019):

- Sınıf içi uygulamalara dijital vatandaşlığın nasıl dahil edileceğini öğrenme
- Dijital vatandaşlık ile ilgili bilgi edinme

- Sınıf müfredatında dijital becerilerin nasıl geliştirileceğini öğrenme
- Öğrencilerin dijital becerilerinin geliştirilmesi amacıyla müfredatta yöntemlerin yer alması
- Dijital okuryazarlığın teşvik edilerek, okulun güvenli öğrenme ortamı durumuna getirilmesi
- Kişinin en iyi uygulamayı ders planına dahil etmesi
- İnternetin ve dijital araçların güvenli kullanımına ilişkin bilgi edinme
- Çeşitli eSafety materyallerini ve kaynaklarını keşfetme, eSafety müfredatının geliştirilmesi.

Selma (Social and Emotional Learning for Mutual Awareness): Şekil 2.13'te görülen "Selma" projesi Avrupa Komisyonu tarafından gerçekleştirilmiş, ortak farkındalık, saygı ve hoşgörüyü teşvik etmek suretiyle dijital ortamda nefret dili sorununu ele almış ve 2017-2019 yıllarında gerçekleştirilmiştir (SELMA, 2019).



Şekil 2.13. Selma (Social and Emotional Learning for Mutual Awareness) (SELMA, 2019)

Projenin ortaklığını Danimarka, Birleşik Krallık, Belçika, Yunanistan ve Almanya oluşturmaktadır. Proje Avrupa Komisyonu tarafından "Haklar Eşitlik ve Vatandaşlık" programı kapsamında 2014-2020 sürecinde desteklenmiştir (SELMA, 2019).

2.2. Dijital Veri

Dijital verilerin oluşturulması, bilgisayar, sunucu, akıllı telefon gibi dijital ortamlarda işlenen, saklanan ve paylaşılan bilgilerin her geçen zaman artması ile veri kavramının günlük yaşamda kalıcı hale gelmeye başladığı söylenebilir. Dijital veri, masaüstü ve dizüstü bilgisayarlar, tabletler, akıllı telefonlar gibi çeşitli teknolojik cihazlar ile her türlü ortamda üretilebilir. Elektronik belgeler, e-kitaplar, e-postalar, dijital

videolar, dijital sesler ve dijital görüntüler dijital verilere örnek gösterilebilir (Yılmaz vd., 2016).

2.2.1. Dijital Veri Güvenliği

İnternet çağı olarak tanımlanan 1990'lı yılların sonlarına doğru verilerin dijital ortamlara transfer edilmesi ve depolanması ile veri güvenliği de önem kazanmaya başlamıştır. McCumber (2005) tarafından "bilgi ve sistemlerinin yetkisiz kullanımı, erişimi, ifşa edilmesi, değiştirilmesi, bozulması veya bilginin bütünlük, gizlilik ve kullanımına zarar verecek kötü niyetli girişimlere karşı yapılan koruma" şeklindeki tanımının günümüz koşullarında da geçerli olabilecek en kapsamlı veri güvenliği tanımı olduğu ifade edilmektedir (Henkoğlu ve Yılmaz, 2013).

Günümüzde internetin sağladığı olanaklar ile bilgi ve veri alışverişinin yer ve zaman kavramı olmadan kolaylıkla yapılabilmesi nedeniyle teknoloji bağımlılığı giderek artmaktadır. İletişim ağları ve bilgisayarların yoğun kullanımı ile birlikte dijital ortamlarda verilerin ve teknolojik güvenliğin önem kazanması söz konusu olmuştur. Elektronik ortamda bilginin üretilmesi, sunumu ve avantajlarının yanı sıra güvenlik sorunları da gündeme gelmiştir. Dijitalleşmenin bu düzeyde artması dijital veri güvenliği risklerini de beraberinde getirmiştir. Dijital veri güvenliği kavramı genel anlamda aşağıdaki gibi özetlenebilir (Kaya ve Öztürk, 2017):

- Gizlilik: Dijital verilerin bir başkası tarafından görüntülenebilir olmamasını istemek. Gizlilik çeşitli şekillerde ihlal edilebilir. Bu bakımdan fiziksel ve internet ortamında gizlilik ilkesinin sağlanması zorunludur. Gizli veriye farklı yollarla erişim olanağı bulunabilir. Örneğin, dijital ortamda paylaşım sırasında şifresiz haberleşme yapılması, hatalı dosyanın gönderilmesi gösterilebilir (Kara 2018, s. 15).
- Bütünlük: Dijital verilerin bir başkası tarafından değiştirilebilir olmamasını istemek. Verilerin yapısının tam olmasının ve doğruluğunun sağlanmasıdır. Veri içeriğinin değiştirilmemiş olması, herhangi bir kısmının ortadan kaldırılmamış veya silinmemiş olması gerekmektedir (Şen ve Yerlikaya 2013).
- Erişilebilirlik: Dijital verilerin yer ve zaman kavramı olmadan ulaşılabilir olmasını, kullanıma hazır olmasını istemek. Güvenlik önlemlerinin veri erişimini zorlaştırması önemli sorunlar arasında görülmektedir. Bu bakımdan erişilebilirlik

ile güvenlik önlemleri arasındaki denge doğru kurulmalı, aşırıya gidilmeden önlemler uygulanmalıdır (Henkoğlu ve Yılmaz 2013).

Dijital güvenlik kavramı genel olarak çevrimiçi veri, kimlik ve diğer varlıkların korunması amacıyla kullanılan kaynakları ifade etmektedir. Bunlar arasında anti virüs yazılımı, web hizmetleri, biyometri, güvenli kişisel cihazlar, akıllı telefon kartları bulunmaktadır. Bunun yanında dijital güvenlik; mobil cihazların, bilgisayarların, internet bağlantısı olan cihazların, tabletlerin, kimlik avı, bilgisayar korsanlığı ve diğer istenmeyen durumlardan korunması anlamını da taşımaktadır (Vigderman ve Turner, 2021). Dijital dünya ve internetin yaşamın her alanındaki etkisi arttıkça kötü amaçlı kullanıcıların hedefi haline gelmiş, veri güvenliğine karşı yapılan saldırılar da artmaya başlamıştır. Bu durum aynı zamanda var olan verinin korunması bakımından sorun haline gelmiştir (Taner ve Kılıç 2019).

Dijital ortamlarda verilerin artması, kişisel verilerin gizliliğine yönelik ihtiyaçtan ve hizmet sağlayıcılara karşı güvenin arttırılmasını gerektiren dijital veri güvenliğine ilişkin sorunların ortaya çıkmasına neden olabilmektedir (Praveena ve Smys, 2017). Dijital ortamlarda bir günde ele geçirilen dijital veri yedi milyonun üzerinde olup, 2020 yılının ilk çeyreğinde suiistimal ve siber dolandırıcılık olaylarında yüzde 20 artış gerçekleşmiştir (Simplilearn, 2021). Bundan dolayı dijital ortamlardaki iletişimde en önemli ve temel sorunlar arasında, internetten iletimi gerçekleştirilen dijital verilerin güvenliği yer almaktadır (Solichin ve Ramadhan, 2017). Genel olarak dijital veri güvenliğinin amacı, verilerin yetkisiz kişiler tarafından ele geçirilmesini, ortadan kaldırılmasını veya yapılarının değiştirilmesini önlemektir (Aslay, Çam ve Özen, 2019, s. 11).

Teknolojiden, süreçlerden ve insanlardan kaynaklanan veri kayıplarının azaltılması için dijital veri güvenliği farkındalığı öne çıkmaktadır (Mediapharm, 2019). Bireyler bu anlamda veri güvenliklerini tehdit edebilecek eylemleri bilinçli olarak yapmamaktadırlar (Gökçearslan, Günbatar ve Sarıtepeci, 2021). Dijital veri güvenliğine ilişkin ihlal ve tehditlerin pek çoğu bireylerin dijital veri güvenliği farkındalığı eksikliklerinden dolayı yaşanmaktadır (Taha ve Dahabiyeh, 2020).

2.2.2. Dijital Veri Güvenliğini Tehdit Eden Unsurlar

Bilişim teknolojilerinde yaşanan gelişmelere paralel bireyler ve kurumlar verilerini saklamak amacıyla dijital ortamları kullanmaya başlamış, ancak verilerin yetkisiz kullanıcıların eline geçmesi telafisi zor sonuçlara neden olmuştur (Keleş ve Güneş, 2013). Teknolojinin sağladığı yararlar beraberinde teknik problemler, bilgisayar virüsleri ve hileleri, yetkili erişimleri kasıtsız veya kasıtlı olarak kötüye kullanma, bilgi hırsızlığı gibi sorunların yaşanmasında etkili olduğu söylenebilir. Dijital veri güvenliğine yönelik tehditler; fiziksel tehditler, insan kaynaklı tehditler, yazılım tehditleri, eğitim ve bilinç eksikliği nedeniyle oluşan tehditler, güvenlik boşlukları şeklinde sınıflandırılabilir (Korucu, 2021):

İnsan Kaynaklı Tehditler: Dijital veri güvenliğine yönelik insan kaynaklı tehditler bilinçli ya da bilinçsiz yapılan girişimler olarak değerlendirilebilir. Kullanıcıların dijital veri güvenliği farkındalıklarının olmaması veya yetersiz olması, dijital sistemlerin yetersiz bilgi ile bilinçsizce kullanımı, veri güvenliği farkındalığı eğitimlerini almamış olmaları insan kaynaklı tehditlere örnek olarak gösterilebilir. Kötü niyetli kullanıcıların zarar vermek amacıyla yaptıkları saldırılar ise bilinçli olarak yapılan tehditler kapsamında ele alınabilir.

Yazılım Tehditleri: Dijital veri güvenliğine yönelik yazılım tehditleri veri kayıplarına neden olabilmektedir. Kötü amaçlı olarak yazılımlar değiştirilebilir, tahrip edilebilir, silinebilir. Yazılımların sistemden veri sızdırmalarının zor fark edilmesinin temel nedeni, yazılımın önceki işini yaparken saldırganın beklentisi olan işlemleri de yapabilmesidir. Bu şekilde veriye istenmeyen programlar veya kişiler erişebilirler.

Güvenlik Zafiyetleri: Dijital veri güvenliğini riske sokan donanım, yazılım veya tasarım hatalarından dolayı oluşan açıklıklardır. Sistemlerdeki güvenlik zafiyetleri trojan, virüs gibi zararlı yazılımlar yardımıyla istismar edilmekte ve veri açıklıkları oluşmaktadır.

Siber Casusluk ve Sürekli Tehditler: Genelde büyük organizasyonlar veya devletler tarafından uzun vadede büyük kaynaklar ile yürütülen veri hırsızlığı siber casusluk ve sürekli tehditler olarak nitelendirilir.

Veri Açıklıkları: Dijital ortamlardaki verilerin istenmeyen şekilde dışarıya sızmasına neden olan durumlardır. Bu durumlar hedef odaklı siber saldırılar, kötü niyetli

kullanıcılar tarafından güvenlik zafiyetlerinin kullanılması veya genelde finansal çıkar amacı olan siber güç kategorisindeki "hack" olaylarını içermektedir.

Mobil Tehditler: Son yıllarda tabletler, cep telefonları gibi mobil platformları etkisi altına alan zararlı yazılımlar kullanıcıların verilerini tehdit etmektedir.

E-Posta Tehditleri ve Spam e-postalar: Bu tehdit amacı dışında kişisel e-posta adreslerinin paylaşılması, kontrolsüz erişim sağlanan web sayfaları üzerinden e-postaların alınması şeklinde ortaya çıkmaktadır.

Bulut Teknolojileri Tehditleri: Bulut bilişim teknolojilerinde son yıllarda siber güvenlik tehditlerinin artmaya başladığı gözlenmektedir. Bulut sistemleri her tür veriyi barındırmaktadır. Dijital platformlarının güvenlik zafiyetleri ve kullanıcıların hatalı kullanımları bulut sistemlerinde dijital veri güvenliği açısından tehdit oluşturabilmektedir.

Sosyal Medya Tehditleri: Son dönemde Twitter, Facebook, Instagram gibi sosyal medya platformlarının yaygın kullanımının siber saldırı tehditlerinin de artmasında etkili olduğu söylenebilir. Sosyal mühendislik saldırıları ve oltalama saldırıları bu platformlara yapılan yaygın saldırı yöntemleri olarak gösterilebilir (Korucu, 2021).

2.2.3. Dijital Veri Güvenliği İhlalleri

Dijital ortamda bireysel ve kurumsal anlamda veri güvenliği ihlallerinin tespiti genelde kolay olmamaktadır. Hatalı veri kullanımının veya verilere yönelik saldırıların tespitinde yükümlülükler, tespit edilen sorunların hangi sistemlerde gerçekleştiği, zararın tespit yöntemi, veri ihlali durumunda yapılacaklar daha önceden belirlenmelidir. Dijital veri güvenliği ihlallerinin belirlenmesinde ve sınıflandırılmasında aşağıdaki adımlar izlenmelidir:

- Dijital veri güvenliği ihlalinin parçası olarak belirlenmiş olan olayların raporlanması, bunların sınıflandırılması amacıyla süreçlerin uygulanması,
- Dijital veri güvenliği ihlalleri kapsamında olayların belirlenmesinde etki, kategori, öncelik, aciliyet gibi etkenlerin belirlenmesi,
- Dijital veri güvenli ihlallerinin yazılım, donanım gibi ilişkili alana göre sınıflandırılması (Korucu, 2021).

Dijital veri güvenliği ihlallerinin takibi ve çözümlenmesi için:

- Dijital veri güvenliği ihlallerinde raporlanan olayların temel nedenlerinin izlenmesi, analizi ve tespitine olanak verecek şekilde denetim izinin oluşturulması,
- Temel nedene yönelik olarak kalıcı çözümlerin belirlenmesi ve bunların başlatılması,
- Çözüm sürecinde hataların ve problemlerin giderilmesi amacıyla işlemlerin düzenli raporlanması.

Dijital veri güvenliği ihlallerinin tespitinde teknolojik çözüm olarak Security Information and Event Management (SIEM) güvenlik bilgi ve olay yönetimi araçları kullanılmaktadır. SIEM tekniği, belirlenmiş kurallar ve politikalar ile bağımsız görünen olayların arasında anlamlı bağlantılar sağlayarak olası saldırıları tespit eden korelasyon tekniğidir. Bu sayede gerçek zamanlı olarak bir ağda bütünsel görünüm sağlanır ve güvenlik tehditlerine yönelik mücadelede proaktif olmak mümkün olabilir (Korucu, 2021).

2.2.4. Dijital Veri Güvenliği Denetimi

Dijital veri güvenliği denetimi, kurumlarda veri ile teması olan her kademenin dahil olduğu ve sorumluluk aldığı bir süreçtir. Denetimin amaca uygun gerçekleştirilebilmesi için gerekli ortam oluşturulmalı, periyodik olarak denetimler gerçekleştirilmelidir. Kurumlarda denetim kontrolleri önleyici, belirleyici, doğrulayıcı ve sorunların çözümüne yönelik kontroller şeklinde sınıflandırılmaktadır (Korucu, 2021, s. 32):

- Önleyici kontroller sırasında genellikle internet güvenlik sistemleri, cihaz konfigürasyonu ve şifreleme, güvenlik duvarları, saldırı önleme sistemleri yaygın olarak kullanılan yöntemler olmaktadır.
- Belirleyici kontroller arasında zafiyet taraması, saldırı tespit sistemleri, olası sorunları ve güvenlik durumlarını belirlemeye yönelik kontroller yer almaktadır.
- Doğrulayıcı ve sorun çözümüne yönelik kontroller arasında ise iş sürekliliği yönetimi, acil durum merkezleri, yama yönetim sistemleri, iş sürekliliği yönetimi sıklıkla kullanılan örnekler arasında yer almaktadır (Korucu, 2021, s. 32).

Bireysel dijital veri güvenliği denetimi ise bilinçli olarak denetimin yapılmasını gerektiren bir süreçtir. Kişisel verilerin korunması ve dijital veri güvenliği bakımından

insan faktörü önem arz etmektedir. Bilgi teknolojilerini, sosyal ağları, mobil cihazları, interneti etkin ve verimli şekilde kullanabilen, platformlardaki verileri korumak amacıyla neler yapması gerektiğinin bilincinde olan kullanıcıların artması, yasal düzenlemeler ve yaptırımlar hakkında bilgi sahibi olunması, veri güvenliğini sağlama veya sorunların azaltılması için faydalı olacaktır. Diğer bir ifade ile bireylerin dijital veri güvenliği farkındalığına sahip olmaları gerekmektedir (Hanaylı, Sebetci, Topal ve Gürel Dönük, 2018, s. 402).

2.2.5. Türkiye'de Dijital Veri Güvenliğini Sağlamaya Yönelik Yasal Düzenlemeler

Teknolojinin gelişmesi, veri güvenliği ihtiyacının artması ile dünyada olduğu gibi Türkiye'de de dijital veri güvenliği gündeme gelmiştir. 2003 yılında başlayan "Dünya Bilgi Toplumu Zirvesi" çalışmaları ele alınmaya başlanmıştır (Şener ve Erdikmen, 2019). Bu doğrultuda 5070 Sayılı "Elektronik İmza Kanunu" oluşturulmuş, devamında 5809 Sayılı "Elektronik Haberleşme Kanunu" ile 5237 Sayılı "Türk Ceza Kanunu" veri güvenliği, bilişim suçları, siber güvenlik alanında önemli adımlar atılmıştır (Coşkun ve Yıldırım, 2019, s. 1560). Aynı zamanda 5651 Sayılı **"**İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi" kanununun yürürlüğe girmesi ile siber suçlarla mücadelede önemli bir gelişme olmuştur (Kılınç, 2016).

Türkiye'de kişisel verilerin korunması ile ilgili olarak başta Anayasa'da olmak üzere farklı kanunlar ile çeşitli düzenlemeler yapılmıştır. Fakat yapılan düzenlemelerin önleyici nitelik taşımaması nedeniyle kişisel verilerin korunması amacıyla bu konunun özel bir kanun ile değerlendirilmesi zorunluğunu doğmuştur (Henkoğlu, 2017).

2.2.5.1. T.C. Anayasası'nın İlgili Maddeleri

Hukuksal olarak temel hak ve özgürlükler, kişisel verilerin korunması, mahremiyet hakkı kavramları, özel hayatın korunması ve gizliliği kapsamında değerlendirilmektedir. Bu çerçevede hazırlanan kanunlar, yönetmelikler, tüzükler ve yasal düzenlemelerin Anayasal hükümler ile uyumlu olması gerekmektedir.

Anayasa'nın ikinci kısmı kişinin temel hak ve ödevlerini düzenlemektedir. Kişinin temel haklarının biri özel hayatın gizliliğidir. Anayasa'nın 20.maddesinde bu hak güvence altına alınmıştır. Temel hak ve hürriyetlere müdahale edilebilmesi teknolojik gelişmelerle daha kolay hale gelmesi ve bunun hukuki bir sorun teşkil etmesi ile birlikte

yasal düzenlemelerin yapılması gerekli olmuştur. Bununla birlikte kişisel verilerin işlenmesine ilişkin düzenlemeler Anayasa'daki özel hayatın gizliliğinin sınırlandırılmasına ilişkin esaslarla uygunluk göstermelidir (Civelek, 2011).

Anayasa'da 5982 Sayılı Kanun ile 2010 yapılan değişiklik ile Anayasa'nın 20.maddesine ek fıkra eklenmiş ve kişisel veriler "Özel hayatın gizliliği ve korunması hakkı" çerçevesinde Anayasa güvencesine kavuşmuştur (Türkiye Cumhuriyeti Anayasası, 1982). Anayasa'daki ek fıkrada **"***Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir"* hükmü yer almaktadır (Ek fıkra: 7/5/2010-5982/2 madde)**.**

Anayasa'da haberleşmenin gizliliği 22.madde ile güvenceye alınmıştır (Türkiye Cumhuriyeti Anayasası, 1982).

Madde 22- (Değişik: 3/10/2001-4709/7 md.)

"*Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.*

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.

İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."

Anayasa'da düşünce ve kanaatleri açıklamaya zorlanamama 25.madde ile güvenceye alınmıştır (Türkiye Cumhuriyeti Anayasası, 1982).

Madde 25- "*Herkes, düşünce ve kanaat hürriyetine sahiptir.*

Her ne sebep ve amaçla olursa olsun kimse, düşünce ve kanaatlerini açıklamaya zorlanamaz; düşünce kanaatleri sebebiyle kınanamaz ve suçlanamaz."

2.2.5.2. Kişisel Verileri Koruma Kanunu

İnternetin tüm dünyaya yayılması ile küresel bir ağ oluşmuş ve kişisel verilere ulaşmak daha kolay hale gelmiştir. Buna bağlı olarak veriler dijital ortamda kıtalar veya ülkeler arasında daha hızlı paylaşılabilir olmuştur. Kişisel verilerin istenmeyen kişilerin eline geçmesi risk olarak görülmektedir. Türkiye'de 6694 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK) 24.03.2016 Tarihli Remi Gazete'de yayımlanmış ve yürürlüğe girmiştir. KVKK 3/d maddesinde yer aldığı üzere kişisel veri; kimliği belirlenebilir veya belirli olan gerçek kişiye yönelik her türlü bilgi olarak hüküm altına alınmıştır. Bu doğrultuda ad-soyad, telefon, e-posta, medeni hal, adres, telefon rehberi, banka hesapları, ses ve görüntü kayıtları, sosyal medya hesapları kişisel veri olarak nitelendirilebilir (Çetin, 2014).

KVKK'nın yürürlük tarihinden önce depolanmış veriler ise Kanun'un yayım tarihinden başlayarak 2 yıl içerisinde Kanun hükümlerine uyumlu hale getirilmelidir. KVKK hükümlerine aykırı olduğu belirlenmiş olan kişisel veriler ise anonim hale getirilir veya yok edilir (Dağsalı, 2019).

2.2.5.3. Sosyal Medya Yasası

5651 Sayılı İnternet Kanun'da değişiklikler yapan ve sosyal medya ile ilgili düzenlemeler getiren 7253 Sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun" başlıklı Kanun 29.07.2020 tarihinde Türkiye Büyük Millet Meclisi'nde (TBMM) kabul edilmiştir (TBMM, 2020).

Sosyal medya alanında düzenlemeler getiren kanunun temel gerekçesi olarak, *"Sosyal ağ sağlayıcılarının geniş çaplı kullanıcı sayıları ile kullanıcı verilerinden elde ettikleri milyarlarca dolar gelire rağmen, kişilerin haklarının korunması noktasında ihtiyaç duyulan önleyici ve koruyucu mekanizmaları geliştirmedikleri ya da etkin kullanmadıkları veyahut devletlerin haklı taleplerine direnç gösterdikleri (...) temel hak ve özgürlüklerin korunması noktasında devletlere düşen pozitif yükümlülüğün yerine getirilmesinde zorlukların"* yaşanması gösterilmiştir. Kanun ile yapılan değişiklikle sosyal ağ sağlayıcılarına getirilen düzenlemelerle kişilik hakları zedelenen bireylere yönelik devletin koruma ve önleme şeklindeki yükümlülüklerini yerine getirmesi amaçlanmaktadır. Fakat Kanun içeriğinde belirlenen amacı aşacak şekilde günümüzdeki

en önemli haber ve bilgi alma kaynağı durumuna gelen sosyal medya ve internetin yasal düzenlemeler ile kuşatıldığı, kişilerin ifade özgürlüğü ile haber alma hakkının engellendiği ölçüsüz birçok yaptırıma yer verildiği belirtilmektedir (Dülger ve Özkan, 2021).

2.2.5.4. Elektronik Haberleşme Sektöründe Veri Güvenliğine İlişkin Düzenlemeler

Elektronik haberleşme sektöründe veri güvenliğine ilişkin yapılan düzenlemeler Elektronik Haberleşme Kanunu ve yönetmelikler olarak ele alınabilmektedir. 5809 Sayılı Elektronik Haberleşme Kanunu, 05.11.2008 Tarihinde kabul edilmiş ve 27050 Sayılı Resmî Gazete'de 10.11.2008 tarihinde yayımlanarak yürürlüğe girmiştir (Elektronik Haberleşme Kanunu, 2008). Kanun, elektronik haberleşme sektöründe kişisel verilerin korunmasına ilişkin hükümler içermektedir. Kanun'un 12/2(d) maddesinde kişisel veri ve gizliliğin sağlanması işletmecilerin hak ve yükümlülükleri arasında belirlenmiştir. Kanun'un 12/2(g) maddesinde ise teknik olarak işletmecilerden yasalarla yetkili olan kurumlar tarafından yasal dinlemenin ve iletişime müdahale yapılmasını sağlamayı temin etme yükümlülüğü düzenlenmiştir.

Bunun dışında Elektronik Haberleşme Kanunu'nda veri güvenliğine ilişkin aşağıdaki maddeler bulunmaktadır.

MADDE 51 – (1) "*Kurum, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkilidir*."

MADDE 55 – (1) "*Kurum tarafından izin verilmedikçe, abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler veya cihazın teşhisine yarayan elektronik kimlik bilgileri yeniden oluşturulamaz, değiştirilemez, kopyalanarak çoğaltılamaz veya herhangi bir amaçla dağıtılamaz.*"

MADDE 56 – (1) "*Abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler ile cihazların elektronik kimlik bilgilerini taşıyan her türlü yazılım, kart, araç veya gereç yetkisiz ve izinsiz olarak kopyalanamaz, muhafaza edilemez, dağıtılamaz, kendisine veya başkasına yarar sağlamak maksadıyla kullanılamaz.*"

Elektronik haberleşme sektöründe hukuki ve teknik alandaki gelişim ve değişimlere yanıt verebilmek amacıyla 2013 yılında "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik"

yayımlanmıştır. Yönetmeliğin amacı 1/1 maddede "*Bu Yönetmeliğin amacı, elektronik haberleşme sektöründe kişisel verilerin işlenmesi, saklanması ve gizliliğinin korunması için elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin uyacakları usul ve esasları düzenlemektir*" şeklinde belirtilmektedir. Ancak Yönetmeliğin 1/1 maddesi gereğince haberleşmenin içeriğine yönelik bilgilerin saklanması kapsam dışında kalmıştır. Yönetmelik, hizmet alanı telekomünikasyon olan gerçek ve tüzel kişileri içermektedir (Kılınç, 2012). Yönetmelikte kişisel verilerin güvenliğine ve iletişimin güvenliğine ilişkin hükümlerle uygulanacak usuller yer almaktadır.

Elektronik Haberleşme Kanunu'na dayanılarak çıkarılan 27655 Sayılı "Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği" ise 28.07.2010 tarihli Resmî Gazete'de yayımlanarak yürürlüğe girmiştir[1]. Yönetmeliğin bazı hükümleri ise 28683 Sayılı 20.06.2013 tarihli Resmî Gazete'de yayımlanarak değiştirilmiştir. Yönetmelik elektronik haberleşme hizmetini alan tüketicinin hak ve menfaatlerinin korunmasını amaçlamaktadır. Yönetmelik kişisel verilerin korunmasını amaçlamasa da sektörde kişisel verilerin özel işleme durumlarına ilişkin veri sahibini koruyan hükümler içerdiği belirtilebilir.

27241 Sayılı 28.05.2009 tarihli Resmî Gazete'de yayımlanan ve yürürlüğe giren Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği, sektörde hizmet verebilecek, altyapı ve şebeke sağlayabilecek işletmelerin yetkilendirilmesine ilişkin usul ve esasların belirlenmesini amaçlamaktadır. Bu işletmelerin hak ve yükümlülükleri arasında kullanıcıların veri gizliliği ve veri güvenliğine ilişkin hükümler de yer almaktadır. Yönetmelikte 19/p maddesinde veri gizliliği ve veri güvenliğine müdahalenin önlenmesine dair düzenleme şu şekildedir: *"İşletmeciler, haberleşme mahremiyeti ve güvenliği ile şebeke güvenliğinin sağlanması ve korunması için, her türlü tedbiri almakla, altyapı ve sistemlerinde teknolojik uyumu sağlamakla, elektronik haberleşmeye ilişkin bilgi, belge ve verilerin gerek korunmasında, gerekse iletilmesinde gizlilik hükümlerine uymak ve kanunla yetkilendirilmiş merci dışında başkasının bu bilgileri elde etmesini önlemekle yükümlüdür. İşletmeci, vereceği elektronik haberleşme hizmeti, şebeke ve*

[1] https://www.resmigazete.gov.tr/eskiler/2010/07/20100728-9.htm, Erişim Tarihi: 27.02.2022.

altyapısında kullanılacak cihazlara, yetkisiz kişilerin erişimini ve bozucu/değiştirici müdahalelerini önlemek amacıyla gerekli tedbirleri almakla yükümlüdür.[2]*"*

Bilgi Teknolojileri ve Kurumu tarafından 4 Aralık 2020 tarihli 31324 Sayılı Resmî Gazete'de yayımlanan "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik" yürürlüğe girmiştir[3]. Elektronik haberleşme sektöründe faaliyeti bulunan işletmelerin kişisel verileri işleme faaliyetlerinin hangi koşullarda gerçekleştirecekleri ve uyması gereken koşullar Yönetmeliğin 5.maddesinde düzenlenmiştir:

- Kişisel verilerin hukuka uygun ve dürüstlük kurallarına göre işlenmesi,
- Kişisel verilerin güncel ve doğru olması,
- Kişisel verilerin meşru, açık ve belirli amaçlar doğrultusunda işlenmesi,
- Kişisel verilerin işlendikleri amaçla sınırlı, ölçülü ve bağlantı olması,
- Kişisel verilerin ilgili mevzuatta veya işlendikleri amaca uygun süre ile muhafaza edilmeleri gerekir[4].

Yönetmeliğin 6. maddesinde ise veri güvenliğine ilişkin düzenleme yapılmıştır. İlgili maddede elektronik haberleşme sektöründeki işletmelerin kullanıcılarına veya abonelerine ilişkin kişisel verilerinin güvenliklerini ve sundukları hizmetlerin güvenirliklerini ulusal ve uluslararası standartlara ve KVKK'ya uygun yerine getirmeleri belirtilmektedir[5].

2.2.5.5. Bankacılık Sektöründe Veri Güvenliğine İlişkin Düzenlemeler

Bankacılık sektörü kişisel verilerin yoğun olarak işlendiği bir sektördür. Dolayısıyla sektörde kişisel verilerin korunması önem arz etmektedir. 5411 Sayılı Bankacılık Kanunu 73.maddesinde yapılan değişiklik ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'te KVKK'nın veri koruma rejiminden farklı uygulamaların benimsendiği görülmektedir (Candemir, 2020).

[2] https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=13078&MevzuatTur=7&MevzuatTertip=5, Erişim Tarihi: 27.02.2022.

[3] https://www.resmigazete.gov.tr/eskiler/2020/12/20201204-13.htm, Erişim Tarihi: 27.02.2022.

[4] https://www.resmigazete.gov.tr/eskiler/2020/12/20201204-13.htm, Erişim Tarihi: 27.02.2022.

[5] https://www.resmigazete.gov.tr/eskiler/2020/12/20201204-13.htm, Erişim Tarihi: 27.02.2022.

25.02.2020 tarihli 31050 Sayılı Resmî Gazete'de yayımlanan ve yürürlüğe giren "Bankacılık Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun" ile 5411 Sayılı Bankacılık Kanunu'ndaki 73.maddesinde yapılan değişiklik ile eklenen hükümler aşağıdaki şekildedir[6]:

MADDE 10- 5411 sayılı Kanunun 73. maddesinin üçüncü fıkrasına ikinci cümlesinden sonra gelmek üzere aşağıdaki cümleler ve maddeye aşağıdaki fıkra eklenmiştir.

"Bankacılık faaliyetlerine özgü olarak bankalarla müşteri ilişkisi kurulduktan sonra oluşan gerçek ve tüzel kişilere ait veriler, müşteri sırrı hâline gelir. Diğer kanunların emredici hükümleri saklı kalmak kaydıyla, müşteri sırrı niteliğindeki bilgiler, bu maddede belirtilen sır saklama yükümlülüğünden istisna tutulan hâller haricinde, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca müşterinin açık rızası alınsa dahi, müşteriden gelen bir talep ya da talimat olmaksızın yurt içindeki ve yurt dışındaki üçüncü kişilerle paylaşılamaz ve bunlara aktarılamaz. Kurul ekonomik güvenliğe ilişkin yapacağı değerlendirme neticesinde, müşteri sırrı ya da banka sırrı niteliğinde olan her türlü verinin, yurt dışındaki üçüncü kişilerle paylaşılmasını ya da bunlara aktarılmasını yasaklamaya, ayrıca bankaların faaliyetlerini yürütmede kullandıkları bilgi sistemleri ve bunların yedeklerinin yurt içinde bulundurulması hususunda karar almaya yetkilidir. Bu maddede belirtilen sır saklama yükümlülüğünden istisna tutulan hâllerde yapılacak paylaşımlar da dâhil olmak üzere, müşteri sırrı ve banka sırrı niteliğindeki bilgiler, sadece belirtilen amaçlarla sınırlı olmak ve ölçülülük ilkesine uygun olarak bu amaçların gerektirdiği kadar veriyi içermek kaydıyla paylaşılabilir."

"Sır niteliğindeki bilgilerin, üçüncü ve dördüncü fıkralar uyarınca yapılacak paylaşım ve aktarımlarına ilişkin kapsam, şekil, usul ve esasları belirlemeye veya bunlara ilişkin sınırlamalar getirmeye Kurul yetkilidir."

Değişiklik öncesinde müşteri sırrı ifadesi Bankacılık Kanunu'nda yer alsa da kavrama ilişkin tanım yapılmamıştır. Müşteri sırrı kavramı Kanun'un 4.maddesinde sayılmış bankacılık faaliyetleri çerçevesinde banka ile hukuki ilişki kuran veya kurmak

[6] https://www.resmigazete.gov.tr/eskiler/2020/02/20200225-12.htm, Erişim Tarihi: 27.02.2022.

üzere olan bireylerin mali, iktisadi, mesleki ve ticari durumlarına ilişkin bankanın edinmiş olduğu her türden bilgiyi, bireylerin faydalandıkları veya faydalanmak istedikleri bankacılık hizmetlerini veya kurulmuş hukuki ilişkiye dair bilgileri kapsamaktadır. Örnek olarak; bankanın kredi verdiği kişilerin mali, ticari, iktisadi durumuna dair edindiği bilgiler yanında kredi başvurusu kabul edilmeyen kişilerin bu tür bilgileri de müşteri sırrı olarak kabul edilmektedir (Alıcı, 2017, s.1289).

2011 yılından itibaren yürürlükte olan Bankaların Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliği'nin yerine 15 Mart 2020 tarihinde 31069 Sayılı Resmî Gazete'de Bankacılık Düzenleme ve Denetleme Kurumu (BDKK) tarafından "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik" kademeli şekilde yürürlüğe konmuştur[7]. Türk bankacılık sektörü teknoloji ve veri güvenliği yatırımı bakımından Türkiye'deki en büyük sektör olup, yeni yönetmelik ile gelişmiş bankacılık sistemine adım atılmıştır. Yönetmeliğin özellikle veri güvenliği konusuna önem vermesi dikkat çekicidir (Korucu, 2021, s. 115).

2.2.5.6. Yüksek Öğretim Kurumu (YÖK) ve Millî Eğitim Bakanlığı'nın (MEB) İlgili Yönetmelikleri

Eğitim faaliyetleri sırasında öğrencilerin belirli amaçlarla başta iletişim ve kimlik verileri olmak üzere kişisel verileri işlenmektedir. Yüksek Öğretim Kurumu (YÖK) ve Millî Eğitim Bakanlığı'nın (MEB) kişisel verileri koruma mevzuatı 6698 Sayılı KVKK hükümlerine uygun olarak düzenlenmiştir. Kanun'da benimsenen terminoloji uyarınca öğrencilerin kişisel verilerinin işlenmesinin araçlarını ve amaçlarını belirleyen, veri kayıt sistemi kurulumu ve yönetiminde sorumlu olan üniversitelerde veri sorumlusudur. Veri işleyen dijital platform sağlayıcıları ise üniversiteden aldığı yetki ile öğrencilerin kişisel verilerini üniversite adına işlemektedir. Öğrenciler ise kişisel verileri işlenen ilgili kişi konumunda olmaktadır. KVKK'nin 5.maddesinde kişisel verilerin işlenme koşullarına yer verilmiştir. Kanun'un 6.maddesinde ise özel nitelikli kişisel verilerin işlenme koşulları düzenlenmiştir. Ancak yasal koşullar ne olursa olsun kişisel veriler KVKK 4.maddesinde düzenlenmiş ilkeler doğrultusunda işlenmelidir (Esenyel Hanaz, 2021).

[7] https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm, Erişim Tarihi: 27.02.2022.

2.2.6. Dünyada Dijital Veri Güvenliğini Sağlamaya Yönelik Yasal Düzenlemeler

Dijital veri güvenliğinin sağlanması amacıyla dünya genelinde kabul görmüş yasal düzenlemeler ve uygulamalar bulunmaktadır. Kişisel verilerin kullanımına yönelik risk ve tehditlerin azaltılması amacıyla dünya genelinde çeşitli yasal düzenlemelere yönelik çalışmalar 1970'li yıllardan itibaren Avrupa Birliği ülkeleri ve Amerika başta olmak üzere ülkelerin pek çoğunda yapılmaya başlanmıştır. Kişisel verilerin korunmasına ilişkin ilk uluslararası belgeler arasında İktisadi İş birliği ve Kalkınma Teşkilatı (OECD) tarafından 1980 yılında düzenlenen OECD Rehber İlkeleri (Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler) bulunmaktadır (Küzeci, 2019, s. 134). OECD Rehber İlkeleri taraf ülkeler açısından bağlayıcı olmayıp, ülkeler takdir yetkisine sahiptirler (Akıncı, 2019, s. 65). Fakat düzenlemenin uluslararası alanda ilk olması nedeniyle dünya genelinde veri güvenliğine ilişkin düzenlemelere ışık olmuş, temel ilkeler hususunda uzlaşı sağlamıştır (Küzeci, 2019, s. 115).

Avrupa Konseyi tarafından 28 Ocak 1981 tarihinde imzaya açılan "108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" 1 Ekim 1985'te yürürlüğe girmiştir. Türkiye'de sözleşmeye taraf olsa da iç hukuka dahil edilebilmesi 17 Mart 2016 tarihinde gerçekleşmiştir. Bundan dolayı Türkiye'de veri güvenliğine ilişkin uygulamalarda sözleşmeye uyulması gerekmektedir. Sözleşme Avrupa Komisyonu üyesi olmayan ülkelerin de sözleşmeyi imzalayabilmeleri ve kişisel veri korumasında uluslararası bağlayıcılığı olmasından dolayı önemli kabul edilmektedir (Küzeci, 2019, s. 126).

Birleşmiş Milletler ise 1990 yılında kişisel verilerin korunmasına ilişkin "Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri" düzenlemesi yapmıştır. Üye ülkeler bakımından yönlendirici olan ilkeler aynı zamanda ülkelerin veri korumaya ilişkin ulusal düzenlemelerinde göz önüne almaları için yayınlanmıştır. Ülkeler açısından bağlayıcı olmayıp, tavsiye niteliği taşımaktadır.

Avrupa Birliği de kişisel verilerin korunmasına ilişkin uluslararası düzeydeki çalışmaların artmasına kayıtsız kalmamış ve 25 Ekim 1995'te "95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi" adı altında düzenlemeyi kabul

etmiştir[8]. Bu düzenleme 2018 yılında "AB Genel Veri Koruma Tüzüğü"nün yürürlüğe girmesi ile yürürlükten kalksa da Türkiye'deki KVKK dahil pek çok ülkenin veri koruma mevzuatına esas oluşturması açısından önem arz etmektedir.

Avrupa Komisyonu tarafından düzenlenen 181 No'lu Protokolde ise taraf devletler ülkelerinde kişisel verilerin korunmasına ilişkin tam bağımsızlıkla görevlerini yerine getirebilecek denetleyici olacak makamları kurma taahhüdü vermişlerdir. Türkiye ise protokolü 8 Kasım 2001'de imzalamış ve 5 Mayıs 2016 tarihli 28703 Sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir[9].

AB Temel Haklar Şartı 2000 yılında Fransa'nın Nice kentinde ilan edilmiştir. Fakat bağlayıcılığı 2009 yılındaki Lizbon Antlaşması ile mümkün olmuştur. AB Temel Haklar Şartı ile kişisel veriler temel hak olarak kabul edilmiş ve AB Hukukunda kişisel verilerin korunması hakkı daha sağlam temellere oturmuştur (Fuster, 2014).

Kişisel verilerin korunması AB Temel Haklar Şartı'nda 8.maddede düzenlenmiştir: *"Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir. Bu veriler, adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak tutulur. Herkes, kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenir."* Düzenlemeye göre kişisel verilerin korunması hakkı temel hak olarak kabul edilmektedir.

2016/679 AB Genel Veri Koruma Tüzüğü ise 1995 yılındaki AB Direktifinin güncellenmiş devamı niteliğindedir. Tüzüğün amacı AB Direktifinde bulunmayan kişisel verilerin korunmasına ilişkin uyumun sağlanmasıdır. Uyum neticesinde ülkeler arasındaki veri akışı daha rahat ve hızlı bir şekilde gerçekleşebilecektir. Teknolojik gelişmelerle birlikte verilerin korunmasına ilişkin ihtiyaç artmıştır. Her geçen zaman kişisel verilerin işlenmesinde yaşanan artış nedeniyle veri paylaşım yoğunluğu da artmıştır. Bu gelişmeler sağladığı faydalar yanında riskleri de beraberinde getirmiştir. Bundan dolayı verilerin gelişmelere paralel etkin şekilde korunması gerekmektedir. Günümüzde internetin yaygınlaşması ve hemen her bireyin sosyal medya hesabına sahip

[8] https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler, Erişim Tarihi: 28.02.2022.
[9] https://www.resmigazete.gov.tr/eskiler/2016/05/20160505.pdf, Erişim Tarihi: 28.02.2022.

olması verilerin korunmasında güncel bir düzenlemenin yapılmasını zorunlu hale getirmiştir (Başalp, 2015). Bu nedenle verilerin korunmasında düzenleme serbestinin üye ülkelere bırakılması yerine ülkelerde bağlayıcı olacak AB Genel Veri Koruma Tüzüğü yürürlüğe sokulmuştur. Tüzüğün kişisel veri konusundaki son düzenleme olması ve bilişim alanındaki gelişmelere uyumlu şekilde düzenlenmiş olmasından dolayı pek çok ülke tarafından kabul görmesinde etkili olmuştur (Başalp, 2015).

2.3. Türkiye'de Yapılan Akademik Çalışmalar

Bu bölümde dijital vatandaşlık ve dijital veri güvenliği farkındalığı ile ilgili Türkiye'de yapılan akademik çalışmalara yer verilmiştir.

2.3.1. Dijital Vatandaşlık ile İlgili Akademik Çalışmalar

Karaduman (2011) yapmış olduğu çalışmada Sosyal Bilgiler dersindeki dijital vatandaşlık etkinliklerinin öğrenme öğretme sürecine ve öğrencilerin dijital ortam tutumlarına etkisini incelemiştir. Çalışma 36 öğrenci ile yürütülmüştür. Çalışmanın sonucunda dijital vatandaşlığı geliştirecek etkinliklerin, katılımcıların güvenlik, gizlilik, sorumluluk, erişim ve haklar tutumlarını ve tutumların kalıcılığını pozitif yönde anlamlı şekilde etkilediği saptanmıştır. Aynı zamanda etkinliklerin katılımcıların dijital tutumlarını olumlu yönde etkilediği, ders başarılarını arttırdığı, kalıcı öğrenmelerine, yorumlama becerilerinin gelişmesine, kavramları somutlaştırmalarına katkı sağladığı bildirilmiştir.

Kocadağ (2012) tarafından yapılan çalışmada öğretmen adaylarının dijital vatandaşlık düzeyleri değerlendirilmiştir. Çalışma 2200 öğretmen adayı ile yürütülmüştür. Katılımcıların dijital vatandaşlık düzeyleri yaş, aile ortalama gelir düzeyi, cinsiyet gibi bazı değişkenler üzerinden anlamlı farklılık olup olmadığı araştırılmıştır. Çalışmanın sonucunda katılımcıların dijital vatandaşlık düzeyleri yüksek bulunmuştur. Cinsiyet değişkenine göre erkek katılımcıların lehine anlamlı farklılık olduğu, aile ortalama gelir düzeyi, yaş değişkenleri ile dijital vatandaşlık düzeyleri arasında da anlamlı farklılık olduğu saptanmıştır.

Kaya ve Kaya (2014) nitel araştırma yöntemi ile yürüttükleri çalışmada Bilgisayar ve Öğretim Teknolojileri Eğitimi (BÖTE) öğrencilerinin dijital vatandaşlık algılarının belirlenmesini amaçlamışlardır. Çalışmanın sonucunda katılımcıların dijital vatandaşlığı tanımlamada vatandaşlık kavramı ile dijital kavramı arasında ilişki aradıkları

görülmüştür. Katılımcılar dijital vatandaşlık ile ilgili okullarda eğitim verilmesini önermişlerdir. Aynı çalışmada katılımcıların tümünün her gün düzenli olarak Twitter, Facebook gibi sosyal ağları kullandıkları, ürün çeşitliliği, zamandan tasarruf etmek ve ürünlerin ucuz olması nedeniyle çevrimiçi alışverişi tercih ettikleri saptanmıştır.

Öztürk (2015) tarafından yapılan çalışmada ortaokul öğrencilerinin dijital vatandaşlık düzeyleri incelenmiştir. Çalışma Kastamonu ilinde 2014-2015 öğretim yılında ortaokul öğrencileri ile yürütülmüştür. Araştırmanın sonucunda katılımcıların bilgi teknolojilerini kullanabildikleri bununla beraber kullanırken yaşanabilecek problemler ile hak ve sorumlulukları hakkında yeterince bilinçli olmadıkları saptanmıştır.

Sakallı (2015) tarafından örnekleminin sınıf öğretmenleri adaylarının oluşturduğu çalışmada katılımcıların dijital vatandaşlık düzeyleri ve siber zorbalık eğilimlerinin arasındaki ilişki incelenmiştir. Çalışmanın sonucunda katılımcıların siber zorbalık eğilimleri ve dijital vatandaşlık düzeyleri yüksek olarak belirlenmiştir. Aynı çalışmada cinsiyet değişkeni ile siber zorbalık eğilimleri arasında anlamlı farklılık olduğu, kadın katılımcıların erkeklere göre siber zorbalık düzeylerinin daha yüksek olduğu belirlenmiştir.

Bakır (2016) tarafından yapılan çalışmada sınıf öğretmeni adayları dijital vatandaşlık düzeyleri dijital vatandaşlık alt boyutlarına göre incelenmiştir. Çalışma 11 sınıf öğretmeni adayı ile nitel araştırma kapsamında yürütülmüştür. Çalışmanın sonucunda katılımcıların dijital vatandaşlık düzeylerinin yüksek olduğu saptanmıştır. Aynı çalışmada bilgisayar tecrübeleri daha iyi olana katılımcıların dijital vatandaşlık düzeylerinin diğer katılımcılara göre daha yüksek olduğu da görülmüştür.

Aslan (2016) yaptığı çalışmada Sosyal Bilgiler öğretmen adaylarının bazı değişkenler bakımından dijital vatandaşlık davranışlarını incelemiştir. Araştırmanın örneklemi Fırat, Siirt, Dicle ve Adıyaman üniversitelerine 2015-2016 eğitim- öğretim yılında Sosyal Bilgiler öğretmenliği bölümünde okuyan 682 öğretmen adayından oluşmuştur. Çalışmanın sonucunda katılımcıların dijital vatandaşlık seviyelerinin yüksek olduğu saptanmıştır. Bunun yanında katılımcıların dijital vatandaşlık seviyeleri ile yaş, cinsiyet, sınıf değişkenlerine göre istatistiksel olarak anlamlı farklılığın olmadığı belirlenmiştir.

Görmez (2016) yaptığı nitel çalışmada dijital vatandaşlık ve boyutlarına ilişkin öğretmen adaylarının görüşlerini ortaya koymayı amaçlamıştır. Çalışma 58 Türkçe Öğretmenliği bölümünde, 68 Sınıf Öğretmenliği bölümünde, 74 Sosyal Bilgiler Öğretmenliği bölümünde eğitim gören öğretmen adayları ile yürütülmüştür. Çalışma sonuçlarına göre; Sosyal Bilgiler Öğretmenliği bölümünün dijital vatandaşlık ve alt boyutlarına ilişkin yeterli bilgiye sahip olmadığı, bunu Türkçe Öğretmenliği ve Sınıf Öğretmenliği bölümünün izlediği görülmüştür.

Som Vural ve Kurt (2018) çalışmalarında dijital vatandaşlık göstergelerinin üniversite öğrencilerinin bakış açısı ile ortaya konmasını amaçlamışlardır. Bu kapsamda geliştirdikleri ölçek yardımıyla dijital vatandaşlık ve alt boyutlarına ilişkin ilişkiler ortaya konmuştur. Aynı çalışmada öğrencilerin üniversite, fakülte, cinsiyet, aylık gelir durumu, internet kullanım sıklığı ile dijital vatandaşlık ve alt boyutlarla ilişkiler de incelenmiştir. Çalışmanın sonucunda katılımcıların cinsiyet değişkeni bakımından dijital vatandaşlık ortalamalarının kadın katılımcılar lehine anlamlı farklılık olduğu, üniversite değişkenine göre anlamlı farklılık olduğu, bununla beraber fakülte değişkenine göre anlamlı farklılık olmadığı saptanmıştır. Çalışmada sınıf düzeyi değişkenine göre dijital vatandaşlık ortalamaları sınıf düzeyinin artmasıyla artmakta olduğu, aylık ortala gelir ve internet kullanım sıklığı arasında anlamlı bir ilişki olduğu da belirlenmiştir.

Çakmak ve Aslan (2018) yaptıkları çalışmada Sosyal Bilgiler öğretmen adaylarının dijital vatandaşlık ve alt boyutlarına ilişkin algılarını incelemişlerdir. Çalışma 361 erkek ve 321 kadın toplam 682 öğretmen adayı ile gerçekleştirilmiştir. Katılımcıların dijital vatandaşlık düzeyleri yaş, cinsiyet, sınıf, aile gelir durumu, kendine ait bilgisayarı olma, sosyal ağ üyeliği, internette kalma süresi değişkenleri üzerinden değerlendirilmiştir. Çalışmanın sonucunda katılımcıların internette kalma süresi ile dijital vatandaşlığa ilişkin tutumları arasında anlamlı farklılık olduğu, internette kalma süresinin artması ile tutumların olumlu yönde değiştiği saptanmıştır. Aynı çalışmada katılımcılar tarafından dijital vatandaş; internet ve bilgisayar kullanmasını çok iyi bilen ve yenilikçi teknolojiye ayak uydurabilen bireyler olarak tanımlanmıştır.

Tatlı (2018) çalışmasında öğretmenlerin dijital vatandaşlık düzeylerini internet ve bilgisayar kullanımı ile bilgi okuryazarlığı öz yeterlilikleri bağlamında değerlendirmiştir.

Çalışmanın sonucunda katılımcıların dijital vatandaşlık düzeyleri ve bilgi okuryazarlığı düzeylerinin arasında pozitif yönlü, orta düzeyde bir ilişki olduğu tespit edilmiştir.

Aydemir (2019) tarafından yapılan çalışmada Sosyal Bilgiler öğretim programı dijital vatandaşlık ve alt boyutları bakımından incelenmiştir. Çalışmada 2017-2018 eğitim öğretim yılında doküman incelemesi yöntemi ile veriler toplanarak, betimsel analiz tekniği ile çözümlenmiştir. Çalışmanın sonucunda Sosyal Bilgiler öğretim programında dijital vatandaşlık ve alt boyutlarına dolaylı ve doğrudan bazı durumlarda yer verildiği ve desteklendiği, bununla birlikte öğrenme alanları ve içerisindeki kazanımların yeterli düzeyde dijital vatandaşlık ve alt boyutlarını yansıtmadığı saptanmıştır.

Dere ve Yavuzay (2019) Sosyal Bilgiler öğretmen adayları ile yürüttükleri çalışmada katılımcıların dijital vatandaşlık göstergelerini incelemişlerdir. Çalışma 401 öğretmen adayı ile gerçekleştirilmiştir. Çalışmanın sonucunda katılımcıların dijital vatandaşlık ölçeği toplam puanları ile günlük internet kullanım süreleri ve okudukları üniversite değişkenlerine göre anlamlı farklılık olmadığı saptanmıştır. Aynı çalışmada katılımcıların e-devlet kullanım sıklığı değişkenine göre gruplar arasında farklılığın anlamlı olduğu belirlenmiştir.

Aldemir ve Avşar (2020) tarafından pandemi sürecinde yapılan çalışmada hükümetler ve kurumların dijitalleşme eğilimleri çerçevesinde dijital vatandaşlık uygulamaları ele alınmıştır. Çalışmanın sonucunda pandemi sürecinde hemen herkesin dijital vatandaş durumuna geldiği ve bunun dijital vatandaşlık kavramının avantajlarını ve dezavantajlarını oluşturduğu görülmüştür. Dijital vatandaşların avantajlar sayesinde yaşamı daha kolay hale gelmekte, özellikle dijital vatandaşlığın okuryazarlık, iletişim ve erişim alt boyutları ile yaşamda doğal akış içerisinde kalabildikleri saptanmıştır.

Güngör ve Kurtipek (2020) yaptıkları çalışmalarında Spor Bilimleri Fakültesi öğrencilerinin yenilikçi düzeylerinin dijital okuryazarlığa olan etkisini incelemişlerdir. Çalışma Ankara ilinde 2019-2020 eğitim öğretim yılında lisans düzeyinde eğitim veren bir yüksek öğretim kurumundaki 205 öğrenci ile yürütülmüştür. Çalışmanın sonucunda katılımcıların kimliklerinin sorgulayıcı yenilikçi oldukları, bununla birlikte dijital okuryazarlık becerilerinin ortalamanın üzerinde olduğu saptanmıştır. Aynı çalışmada dijital okuryazarlık düzeyinin erkek katılımcıların kadın katılımcılardan anlamlı olarak

yüksek olduğu, bireysel yenilikçiliğin %37 oranında dijital okuryazarlığı açıkladığı belirlenmiştir.

Arcagök (2020) tarafından yapılan çalışmada farklı branşlardaki öğretmenlerin dijital vatandaşlık algıları incelenmiştir. Çalışma 215 öğretmen ile yürütülmüştür. Çalışma sonucunda katılımcıların orta düzeyde dijital vatandaşlık algıları olduğu tespit edilmiştir. Aynı çalışmada branş değişkenine göre katılımcıların dijital vatandaşlık algılarının farklılaşmadığı, erkek katılımcıların kadın katılımcılara göre dijital vatandaşlık algılarının daha yüksek düzeyde olduğu saptanmıştır. Çalışmada 1-5 yıl mesleki kıdemde olan katılımcıların diğerlerine göre dijital vatandaşlık algılarının daha yüksek olduğu da bildirilmiştir.

Kaya (2020) çalışmasında ortaöğretim öğrencilerinin dijital okuryazarlık ve dijital vatandaşlık düzeylerinin arasındaki ilişkiyi incelemiştir. Çalışmanın örneklemini Konya ili Selçuklu ilçesinde eğitim gören 847 öğrenci oluşturmuştur. Çalışmanın sonucunda katılımcıların dijital okuryazarlık ve dijital vatandaşlık düzeylerinin yüksek olduğu belirlenmiştir. Aynı zamanda cinsiyete göre kızların dijital okuryazarlık düzeyleri erkeklere göre daha yüksek bulunmuştur.

2.3.2. Dijital Veri Güvenliği Farkındalığı ile İlgili Yapılan Çalışmalar

Tekerek ve Tekerek, (2013) tarafından ilköğretim ve lise öğrencileri ile yürütülen çalışmada katılımcıların bilgisayar ve bilgi güvenliği farkındalık düzeyleri incelenmiştir. Çalışma Kahramanmaraş ilinde 2449 öğrenci ile gerçekleştirilmiştir. Çalışmanın sonucunda katılımcıların bilgi güvenliği farkındalık düzeylerinin yeterli olduğu belirlenmiştir. Bununla birlikte bilgi gerektiren hususlarda ve kurallarda farkındalık düzeylerinin daha düşük olduğu görülmüştür. Bu durum ise bilgisayar ve bilgi güvenliği farkındalık etkinlikleri ve eğitimin yetersiz kaldığı yönünde yorumlanmıştır.

Kınay, Sözcü, Taşkın ve İpek (2014) yaptıkları çalışmada "Bilgi Güvenliği Farkındalığı Ölçeği" geliştirmişlerdir. Çalışma İstanbul ilinde 326 üniversite öğrencisi ile yürütülmüştür. Ölçekte davranış, eğitim ve bilgi düzeylerinde 32 madde yer almakta olup, ölçekten alınacak toplam puanların 60 ve altında olması "düşük" farkındalık düzeyi, 60-69 puan arası orta" farkındalık düzeyi, 80 ve üzerinde "yüksek" farkındalık düzeyi olarak belirlenmiştir. Çalışmanın sonucunda bilgi güvenliği farkındalık düzeyleri için hangi kararların alınması gerektiği tartışılmıştır.

Dönmez, Odabaşı, Kabakçı Yurdakul, Kuzu ve Girgin (2014) tarafından yapılan çalışmada öğretmen adaylarına çocukların karşı karşıya kaldıkları internet risklerine ilişkin algı ölçeği geliştirilmiştir. Sınıf öğretmeni adayları ile ölçeğin geçerlik ve güvenirlik çalışmaları yapılmıştır. Çalışma 392 öğrenci ile yürütülmüş, faktör analizleri yapılmıştır. Yapılan analizlerin sonucunda 20 maddeden ve 6 faktörden oluşan yapıya ulaşılmıştır. Faktörler; internet hesaplarının korunması, zararlı içerikleri, siber zorbalık, cinsellik, zararlı iletişimler ve kişisel bilgilerin korunması olarak tanımlanmıştır. Yapılan çalışmanın sonucunda ortaya konulan yeni ölçme aracı ile öğretmenlerin internet risklerine yönelik algılarının ölçülmesi sağlanabilmiştir.

Arıtürk (2015) tarafından yapılan çalışma 218 Mühendislik Fakültesi öğrencisi ile gerçekleştirilmiştir. Çalışmada katılımcıların bilgi güvenliği ile bilgi farkındalığı incelenmiştir. Çalışmanın sonucunda kadın katılımcıların bilgi güvenliği ile bilgi farkındalığı erkek katılımcılardan daha yüksek olduğu saptanmıştır. Aynı çalışmada branş ve sınıf öğretmenlerinin arasında dijital veri güvenliği farkındalığı bakımından anlamlı farklılık olmadığı görülmüştür.

Yılmaz, Şahin ve Akbulut (2016) yaptıkları çalışmada öğretmenlerin dijital veri güvenliği farkındalıklarını incelemişlerdir. Çalışma 870 öğretmen ile yürütülmüştür. Çalışmanın sonucunda katılımcıların dijital veri güvenliği farkındalık düzeylerinin yüksek olduğu saptanmıştır. Ayrıca katılımcıların farkındalık düzeylerinin günlük internet ve bilgisayar kullanım süresi, cinsiyet, sahip olunan teknolojilere göre değişim gösterdiği, öğrenim kademesi, branş, mesleki kıdem ve öğrenim durumuna göre değişiklik göstermediği görülmüştür.

Sağır, Doğruluk, Mutluay ve Emlik (2018) tarafından yapılan çalışmada katılımcıların bilgi güvenliği farkındalık düzeylerinin belirlenmesi, bazı değişkenlere göre değerlendirilmesi amaçlanmıştır. Çalışma Meslek Yüksekokulu öğrencisi olan 1621 öğrenci ile yürütülmüştür. Araştırmadan elde edilen bulgulara göre katılımcıların orta düzeyde bilgi güvenliği farkındalık düzeylerine sahip oldukları belirlenmiştir.

Korkmaz (2018) tarafından yapılan çalışmada üniversite öğrencilerinde dijital veri güvenliği bilincinin düzeyi belirlenmesi amaçlanmıştır. Çalışma anket tekniği ile yürütülmüştür. Katılımcıların dijital veri güvenliği bilinci düzeyleri belirlenmiştir.

Çalışmadan elde edilen bulguların bu alanda eksikliğin giderilmesine katkıda bulunacağı, uygulamaya ve alan yazına faydalı görüşler sunacağı düşünülmüştür.

Avcı ve Oruç (2020) tarafından üniversite öğrencileri ile yürütülen çalışmada, katılımcıların bilgi güvenliği farkındalıkları ve bireysel siber güvenlik davranışları incelenmiştir. Çalışma 88 üniversite öğrencisi ile yürütülmüştür. Çalışmanın sonucunda elde edilen bulgulara göre bireysel siber güvenlik sağlama ve bilgi güvenliği farkındalıkları altı boyutlarının arasındaki ilişkinin yüksek düzeyde olduğu görülmüştür. Aynı çalışmada farkındalığı düşük olan veya olmayan katılımcılar da olduğu da saptanmıştır. Bunun sosyal medya hesabı sayısı ve bölümlere göre farklılık gösterdiği belirlenmiştir. Öğrencilerin farkındalık düzeylerinin arttırılması amacıyla eğitim programlarına konu ile ilgili derslerin konulması, bireylerin bilinçlendirilmesi, siber güvenlik farkındalıklarının sağlanmasının gerekliliği önerilerinde bulunulmuştur.

Göldağ (2021) tarafından ilişkisel tarama modelinde yürütülen çalışmada üniversite öğrencilerinin dijital okuryazarlık ile dijital veri güvenliği farkındalığı düzeyleri arasındaki ilişki incelenmiştir. Çalışma 265 üniversite öğrencisi ile gerçekleştirilmiştir. Çalışmanın sonucunda öğrencilerin orta düzeyde dijital okuryazarlık düzeylerine, yüksek düzeyde dijital veri güvenliği düzeylerine sahip oldukları görülmüştür. Aynı çalışmada erkek katılımcıların dijital okuryazarlık ile dijital veri güvenliği farkındalığı düzeylerinin kadın katılımcılardan daha yüksek olduğu, ön lisans ve lisans düzeyindeki katılımcıların dijital okuryazarlık ile dijital veri güvenliği farkındalığı düzeyleri arasında farklılık olmadığı, bilgisayar sahibi olan katılımcıların dijital okuryazarlık ile dijital veri güvenliği farkındalığı düzeyleri farkındalıklarının yüksek olduğu, bilgisayar kullanım süresi daha uzun olan katılımcıların ise kullanmayanlara göre dijital okuryazarlık ile dijital veri güvenliği düzeylerinin daha yüksek olduğu saptanmıştır. Ayrıca katılımcıların dijital cihaz kullanma düzeylerinin artması ile dijital okuryazarlık ve dijital veri güvenliği farkındalığı düzeylerinin de arttığı, katılımcıların dijital okuryazarlık ile dijital veri güvenliği farkındalığı düzeyleri arasında pozitif yönde anlamlı bir ilişkinin olduğu bildirilmiştir.

Talan ve Aktürk (2021) yapmış oldukları çalışmada lise öğrencilerinde dijital bilgi güvenliği farkındalık ve dijital okuryazarlık düzeyleri incelenmiştir. Aynı çalışmada katılımcıların cinsiyet, sınıf düzeyi, yaşadıkları şehir değişkenlerine göre bilgi güvenliği

farkındalıkları da ele alınmıştır. Çalışmanın sonucunda katılımcıların dijital okuryazarlık düzeyleri ve bilgi güvenliği farkındalıklarının arasında pozitif yönde ilişki olduğu saptanmıştır. Ayrıca erkek katılımcıların kadın katılımcılara göre bilgi güvenliği farkındalık düzeylerinin daha yüksek olduğu görülmüştür.

Gündüzalp (2021) yapmış olduğu çalışmasında üniversitelerde bilgi işlem daire başkanlığı çalışanlarında siber güvenlik ve dijital veri güvenliği farkındalıklarının belirlenmesini amaçlamıştır. Kesitsel tarama modeli ile yürütülen çalışmada katılımcıların siber güvenlik ve dijital veri güvenliği farkındalıklarının arasında pozitif yönde zayıf ilişki olduğu belirlenmiştir. Aynı çalışmada katılımcıların siber güvenlik ve dijital veri güvenliği farkındalıklarının mesleki deneyim, yaş, görev ve eğitim durumu değişkenlerine göre anlamlı şekilde farklılaştığı görülmüştür. Katılımcıların siber güvenlik ve dijital veri güvenliği farkındalıklarının yüksek olduğu, yaş, cinsiyet, eğitim durumu, görev, mesleki deneyimin farkındalıklar üzerinde etkili olduğu saptanmıştır.

2.4. Yurtdışında Yapılan Akademik Çalışmalar

Bu bölümde dijital vatandaşlık ve dijital veri güvenliği farkındalığı ile ilgili yurtdışında yapılan akademik çalışmalara yer verilmiştir.

2.4.1. Dijital Vatandaşlık ile İlgili Akademik Çalışmalar

Hollandsworth, Dowdy ve Donovan (2011) yürüttükleri çalışmalarında dijital vatandaş sorumluluğuna sahip olmayan öğrencilerin eğitim ortamında yaratabileceği istenmeyen ve tehlikeli davranışlarını incelemişlerdir. Çalışmanın sonucunda elde edilen bulgular doğrultusunda eğitimcilere öğrencilerin iyi dijital vatandaş olarak yetiştirilmeleri için önerilerde bulunulmuştur.

Oyedemi (2012) tarafından yapılmış çalışmada Güney Afrika'da üniversite öğrencileri dijital vatandaşlık ve internet kullanımları bakımından incelenmiştir. Araştırmacı tarafından dijital vatandaşlık yeniden değerlendirilmiş, internet kullanımı, politika, internet yetenekleri, vatandaşlık hakları ve dijital yetenekler olarak beş boyut oluşturularak, kuramsal çerçeveye göre ölçek hazırlanmıştır. Araştırmada Güney Afrika'da kentsel ve kırsal bölgelerindeki 10 üniversiteden veriler toplanmıştır. Çalışmanın sonucunda katılımcıların yeterli dijital vatandaşlık düzeylerine sahip olmadıkları saptanmıştır. Aynı çalışmada internete yetersiz erişimden dolayı etkili

internet kullanımının yeterli olmadığı, bundan dolayı katılımcıların dijital araçları etkin kullanamadığı saptanmıştır.

Lyons (2012) yaptığı çalışmasında öğrencilerin dijital vatandaşlık davranışlarını sınıf düzeyi ve cinsiyet değişkenlerine göre incelemiştir. Çalışmada 2000 öğrenci katılımcı olarak yer almıştır. Çalışmanın sonucunda ölçek alt boyutlarının cinsiyet ile sınıf düzeyi değişkenleri arasındaki farklılığın anlamlı olduğu saptanmıştır. Sınıf düzeyinin yükselmesi ve ebeveyn katılım düzeyinin azalmasıyla bireysel güvenlik risklerinin, dijital zorbalık eğilimlerinin ve dijital vatandaşlık ihlallerinin arttığı görülmüştür. Aynı çalışmada erkek katılımcıların bireysel güvenlik ve dijital vatandaşlık sorunlarının kız katılımcılara göre yüksek olduğu belirlenmiştir.

Suppo (2013) çalışmasında Pensilvanya'da okullardaki yöneticilerin dijital vatandaşlık eğitim uygulamalarına ilişkin görüşleri ve dijital vatandaşlık uygulamalarını ele almış ve okul yöneticilerinin dijital hak ve sorumluluk boyutunu öncelikli olarak öğrencilere öğretmeleri gerektiğini belirtmiştir. Okul yöneticilerinin daha sonra dijital güvenlik, dijital okuryazarlık, erişim, etik, kanun alt boyutlarını benimsetmesi gerektiğini ifade etmiştir. Aynı çalışmada dijital dünyanın et6kisiyle siber suçlarda artış gözlendiğini, eğitimcilerin de bireyleri iyi dijital vatandaş olarak yetiştirme görevlerinin bulunduğu vurgulanmıştır.

Sorbring (2014) çalışmasında ebeveynlerin çocuklarının internet kullanımına ilişkin endişe ve kaygılarını araştırmıştır. Çalışmada ebeveynlerin kaygı ve endişelerinin çocuklarının cinsiyet ve yaşına bağlı olarak değişiklik gösterdiği saptanmıştır. Ebeveynlerin kendi internet kullanım deneyimleri, internet becerileri, internet kaygıları ve endişelerinin türü ve doğası ile ilişkilidir. Çalışmanın sonucunda ebeveynler üç gruba ayrılmıştır. Gruplardan biri internetin üstünlüğü yanında sınırlılıkları vardır diyenler, diğeri internetin sınırlılıkları üstünlüklerine göre çoktur, son grup ise internetin üstünlükleri sınırlılıklardan daha fazladır diyenlerden oluşmaktadır. Gruplar arasından internetin sınırlılıkları üstünlüklerinden daha fazladır diyenler daha kaygılı oldukları saptanmıştır. Dijital araçlar hakkında endişeli ve kaygılı olanların ise çocuklarının araçları kullanması konusunda sınırlama getirmelerinin daha yaygın olduğu görülmüştür.

Berardi (2015) çalışmasında farklı branşlarda görev yapan öğretmenlerin dijital vatandaşlık algısını incelemiştir. Çalışmanın sonucunda elde ettiği bulgulara göre sınıf öğretmenlerinin dijital vatandaşlık hususunda en yeterli grup olduğu görülmüştür.

Jones ve Mitchell (2016) yaptıkları çalışmada dijital vatandaşlık konusunda bir ölçek geliştirmişlerdir. Bu ölçeği kullanarak yapmış oldukları araştırmada, katılımcıların yaş düzeyi düştükçe dijital ortamlarda saygılı davranış tutumlarında azalma olduğu belirlenmiştir. Aynı çalışmada dijital vatandaşlık ölçeğinden kız katılımcıların erkek katılımcılara göre daha yüksek puan aldıkları bildirilmiştir.

Netwong (2016) çalışmasında çevrimiçi platform olan Moddle sistemini dijital vatandaşlık eğitiminde kullanmıştır. Bu çalışma ile dijital vatandaşlık eğitimi üzerine araştırma yürütmüştür. Çalışmanın sonucunda katılımcıların akademik başarı düzeyi ile dijital vatandaşlık arasındaki ilişkinin yüksek düzeyde olduğu bildirilmiştir.

Choi, Glassman ve Cristol (2017) tarafından genç bireylerin internet düzeylerini, internet tabanlı gruba katılma yeteneklerini ve algılarını ölçmek amacıyla dijital vatandaşlık alt boyutlarını kapsayan detaylı bir dijital vatandaşlık ölçeği geliştirmek için bir çalışma yürütülmüştür. Dijital vatandaşlığın alt boyutlarının belirlenmesi, geçerlik ve güvenirlilik değerlendirilmesi amacıyla faktör analizleri ile ilişkisel analizler yapılmıştır. Çalışma sonucunda dijital vatandaşlık ölçeği ile öğrencilerin algılarını, internet tabanlı gruba katılım düzeylerini, yeteneklerini farklı boyutlarda ölçmüştür. Ölçeğin öğrencileri bilgilendirmek, etkin dijital vatandaşlar olmalarını sağlamak, eğitmek, dijital vatandaşlık düzeyini yükseltmek için gereken koşulları sağlamada önemli etkileri bulunduğu vurgulanmıştır.

Wisniewski, Xu, Rosson ve Carroll (2017) yapmış oldukları çalışmada çevrimiçi risk deneyimleri açısından çocuklar incelenmiştir. Çalışmanın sonucunda çocukların büyük bir kısmının çevrimiçi riskle karşılaştıklarında ebeveynlerle ilişkilerinin oldukça az olduğu görülmüştür. Ebeveynler farklı yollarla izleme davranışlarını ve aktif arabuluculuğu sergilediklerini belirtseler de çocuklar tarafından ebeveynlerin sınırlı arabuluculuğunun tercih edildiği belirlenmiştir. Aynı çalışmada çevrimiçi risklerle karşılaşan çocukların ebeveynleri ile iletişim kurmama nedeninin ebeveynlerin sınırlı arabuluculuğu olduğu vurgulanmıştır.

Choi, Cristol ve Gimbert (2018) yaptıkları çalışmada hangi faktörlerin öğretmenlerin dijital vatandaşlık düzeylerini etkilediğini belirlemeyi amaçlamışlardır. Çalışmanın sonucunda öğretmenlerin dijital vatandaşlık düzeylerinin internet hususunda kendilerine güvenmeleri, mesleki deneyimleri, sosyal medya kullanmalarının etkili olduğu görülmüştür.

2.4.2. Dijital Veri Güvenliği Farkındalığı ile İlgili Yapılan Çalışmalar

Kruger, Drevin ve Steyn (2010) tarafından yapılan çalışmada üniversite öğrencilerinin bilgi güvenliği farkındalıklarını ölçme aracı geliştirilmesi amaçlanmıştır. Çalışmada farkındalık programlarında yer verilebilecek uygun konuların ve alanların belirlenmesi amacıyla "Bilgi güvenliği sözcük testi" geliştirilmiştir. Sözcük testinin sınanması ve uygulanabilmesini göstermek amacıyla iki bölümden meydana gelen anket kullanılmıştır. Anketin ilk bölümünde sözcük testi, ikinci bölümünde ise katılımcıların davranışlarının belirlenmesi hedeflenmiştir. Çalışmanın sonucunda bireylerin bilgi güvenliği farkındalığının değerlendirilmesi için sözcük testinin kullanılmasının faydalı olacağı saptanmış, davranışlar ile sözcük bilgisi arasındaki ilişkinin anlamlı olduğu görülmüştür.

Haeussinger ve Kranz (2013) yürüttükleri çalışmada bilgi güvenliği farkındalığını tanımlamada güvenlik sorunlarına ilişkin bilgi ve bilinç durumu ifadesini kullanmışlar ve bunun güvenlik ile uyumlu davranışları sıklıkla etkilediğini bildirmişlerdir. Çalışma bilgi güvenliği farkındalığına etki eden faktörler ve bunların davranışlar üzerindeki etkileri üzerine yürütülmüştür. Çalışmada bilgi güvenliği farkındalığının bireysel, kurumsal ve çevresel öncüllerini kapsayan araştırma modeli önerisi yapılmış, deneysel olarak model test edilmiştir. Çalışmadan elde edilen bulguların bilgi güvenliği araştırmacıları ve yöneticileri bakımından önemli bir etkisi bulunmaktadır. Farkındalığın en önemli öncüllerinin bilgi güvenliği sistemlerinin güvenliğine yönelik bilgi verilmesinin ve tanıtımının olduğu belirtilmiştir. Bu kapsamda kullanıcıların bilgi güvenliği farkındalığını sağlamanın ekonomik, etkili ve daha kolay yolunun kullanıcılar için herhangi bir zamanda çevrimdışı kolay erişilebilen ve anlaşılabilir olan yöntemlerin geliştirilmesi gerekir. Çalışmanın sonucunda bireysel olarak bilgi güvenliği bilgisine sahip olmanın farkındalığın temel belirleyicisi olduğu saptanmıştır. Aynı zamanda kullanıcıların cinsiyet değişkeninin ve tecrübesinin farkındalığa etkili olduğu, kadınların, tecrübesi fazla olanların bilgi güvenliğine daha fazla niyet sergiledikleri görülmüştür.

Farooq, Isoaho, Virtanen ve Isoaho (2015) yapmış oldukları çalışmada üniversite öğrencilerinin bilgi güvenliği farkındalığını ele alarak, çeşitli faktörlerin bu farkındalığı ne şekilde etkilediğini analiz etmişlerdir. Bilgi güvenliği farkındalığını ise davranış ve bilginin kombinasyonu olarak görmüşlerdir. Cinsiyet, eğitim alanı, yaş, eğitim düzeyi, yaşam alanı, uyruk, bilgi güvenliği farkındalığı eğitimi, iş deneyimi gibi faktörler ise bireysel faktörler olarak kabul edilmiştir. Araştırmacılar öğrencilerin arasındaki algılanan bilgi güvenliği farkındalığı düzeyini incelemişlerdir. Çalışmanın sonucunda yaşam alanı, bilgi güvenliği eğitimi, cinsiyet ile bilgi güvenliği farkındalık düzeyinin arasında istatistiksel anlamlı ilişki olduğu saptanmıştır. Bunun yanında uyruk, yaş, eğitim düzeyi, yaş gibi faktörlerle bilgi güvenliği farkındalık düzeyinin arasında anlamlı ilişki bulunamamıştır. Aynı çalışmada eğitim ve cinsiyet, bilgi güvenliği farkındalığı ile algılanan bilgi güvenliği farkındalığının arasında istatistiksel olarak anlamlı bir ilişki olduğu belirlenmiştir.

Tsohou, Karyda ve Kokolakis (2015) yürüttükleri çalışmalarında kültürel ve bilişsel önyargıların bilgi güvenliği politikalarında içselleştirilmesinde rolünü incelemişlerdir. Çalışmanın sonucunda bilgi güvenliği bilinçlendirme programlarında uygulama ve standartların bireylerin güvenliğe yönelik bilgilerini nasıl içselleştirdiklerini, güvenlikle ilgili kararlarını nasıl aldıklarını gözetmeden programların süreçlerine ve içeriklerine odaklandıkları belirtilmiştir.

Öğütçü, Testik ve Chouseinoglou (2016) yapmış oldukları çalışmada kişisel bilgi güvenliği farkındalığının ve davranışlarını analiz etmişlerdir. Çalışmada katılımcıların yük farkındalık düzeyine sahip olmadıkları, bireysel olarak koruyucu davranışların henüz gelişmediği saptanmıştır. Aynı çalışmada katılımcıların siber suçlara maruz kalma oranının oldukça düşük olduğu, eğitim alanların farkındalığının eğitim almayanlara oranla daha yüksek olduğu görülmüştür. Elde edilen bulgulara göre; katılımcıların mevcut tehditleri algıladıkça davranışlarının daha koruyucu duruma geldiği görülmüştür. Katılımcıların tehdit algıları ile riskli davranışları arasında pozitif ilişki olduğu saptanmıştır.

Jeske ve Van Schaik (2016) dijital tehditlerin güvenlik davranışlarının ve internet tutumlarının tahmin edicileri olduğunu ileri sürmüşler ve bir çalışma yapmışlardır. Çalışma 323 üniversite öğrencisi ile yürütülmüştür. Katılımcılara sunulan internet

tehditlerinin ne anlama geldiği, bu tehditleri ne kadar bildikleri sorulmuştur. Elde edilen sonuçlara göre üç grup oluşturulmuştur. Tehditlerin tamamını bilen grupta yer alan katılımcıların diğerleri göre güvenlik duvarı, antivürüs, yazılım güncellemeleri, anticasus yazılımı gibi bilgisayar güvenliği davranışları gösterdiği, internette geçirilen süre ve internet deneyimlerinin fazlalığının tehditlerin bilinirliğinin önemli yordacıları oldukları belirlenmiştir.

McCormac, Zwaans, Parsons, Calic, Butavicius ve Pattinson (2017) tarafından yapılan çalışmada bireysel özellikler çerçevesinde bilgi güvenliği farkındalığı incelenmiştir. Çalışmada bilgi güvenliği farkındalığı ile kişilik, cinsiyet, yaş, risk alma eğilimi gibi bireysel değişkenler arasındaki ilişkinin incelenmesi amaçlanmıştır. Bilgi güvenliği farkındalığı, bireylerin tutum ve davranışları, hangi prosedürleri ve politikaları izlemeleri gerektiği üzerinden incelenmiştir. Çalışmanın sonucunda duygusal istikrarın, anlaşılabilirliğin, risk alma eğiliminin, vicdanlılığın bireylerin bilgi güvenliği farkındalıklarının arasında farklılıkları açıkladığı, cinsiyet ve yaş değişkeninin ise farklılıkları açıklamadığı belirlenmiştir.

Parsons, Calic, Pattinson, Butavicius, McCormac ve Zwaans (2017) tarafından yapılan çalışmada 112 üniversite öğrencisi ile çevrimiçi ortamlardaki bilgi güvenliği davranışlarına ilişkin sormaca geliştirilmiştir. Aynı çalışmada katılımcılar siber atak ortamı düzenlenen bir deneye de katılmışlardır. Sormaca içerisinde e-posta kullanımı, sosyal medya kullanımı, şifre yönetimi, rapor bildirme, bilgi ile başa çıkma, mobil araç kullanımı gibi alanlar bulunmaktadır. Çalışmanın sonucunda yüksek skorları bulunan katılımcıların deneydeki performanslarının daha iyi olduğu belirlenmiş, bundan dolayı sormacanın bilgi güvenliği davranışlarının tahmin edebildiği görülmüştür. Sormaca daha sonra 531 yetişkine uygulanarak, ölçek geliştirmede güvenirlik ve geçerlik çalışmaları yürütülmüştür. Bu çalışmada ilk çalışmada ulaşılan yapıya ulaşılmıştır.

Van Schaik, Jeske, Onibokun, Coventry, Jansen ve Kusev (2017) yürüttükleri çalışmada 436 üniversite öğrencisinin 16 dijital güvenlik zararı çerçevesinde çevrimiçi risk alma algıları ile tehditlerden kaçınma davranışları incelenmiştir. Katılımcıların kimlik hırsızlığını en riskli dijital tehlike olarak, e-posta edinmek ve çerezleri ise en riskli dijital tehlike olarak algıları belirlenmiştir. Çalışmada katılımcıların önemli bir kısmının işletim sistemi güncellemeleri, antivürüs yazılımı kullanma, güvenlik yazlımı kurma gibi

bazı dijital güvenlik beceri düzeylerinin yüksek olduğu saptanmıştır. Bireylerin genelde daha önce yaşadıkları dijital güvenlik ile ilgili olumsuz deneyimlerinin risk algılarını daha fazla arttırdığı görülmüştür.

Gratian, Bandi, Cukier, Dykstra ve Ginther (2018) tarafından yapılan çalışmada bireysel özellikler ile siber güvenlik davranış niyetleri arasındaki ilişkiler incelenmiştir. Çalışma 369 üniversite öğrencisi, idari personel ve öğretim üyesinden oluşan katılımcılar ile gerçekleştirilmiştir. Katılımcıların karar verme stilleri, kişilik özellikleri, risk alma tercihleri, demografik özelliklerinin şifre üretimi, araç güvenliği, güncelleme güvenlik davranışları niyetleri, önleyici farkındalıkları üzerinde çalışma yürütülmüştür. Çalışmanın sonucunda katılımcıların kullandıkları dijital araçların güvenliği ve risk alma tercihleri arasında ilişki olmadığı görülmüştür. Demografik özelliklerinin ise şifre belirleme davranışı üzerinde öngörücü olduğu ortaya konmuştur. Cinsiyet değişkeninin ise farkındalık güvenlik davranışı üzerinde öngörücü olduğu saptanmıştır. Benzer bulguya güncelleme güvenlik davranışı niyetinde de ulaşılmıştır. Özellikle rasyonel karar verme, cinsiyet ve finansal risk alma gibi kişisel özelliklerin iyi güvenlik davranışı niyetleri üzerinde önemli yordayıcı olduğu bildirilmiştir.

BÖLÜM 3

YÖNTEM

3.1. Araştırmanın Modeli

Üniversite öğrencilerinin dijital vatandaşlık bağlamında dijital veri güvenliği farkındalığı düzeylerinin incelendiği tez çalışmasında, nicel araştırma modelinden yararlanılmıştır. Araştırmada nicel araştırma modelleri arasında yer alan betimsel tarama yöntemi kullanılmıştır. Betimsel araştırmalar, bir durumun aydınlatılması amacıyla, değerlendirmelerin belli standartlar kapsamında yapılması ve olaylar arasındaki ilişkinin belirlenmesi için yürütülmektedir (Büyüköztürk vd., 2015). Karasar'a (2020) göre ise, geçmişte gerçekleşen veya hâlihazırda devam eden herhangi bir durumu olduğu gibi ortaya koymayı amaçlayan bir modeldir.

3.2. Çalışma Grubu

Araştırmanın çalışma grubunu Trakya Üniversitesi'nin ön lisans, lisans ve lisansüstü kademelerinde öğretim gören 2500 öğrenciden oluşmaktadır. Ancak anket formunun eksik ya da hatalı doldurulmasından dolayı 6 öğrenci değerlendirme dışı bırakılmış ve 2494 öğrenci değerlendirmeye alınmıştır. Öğrenciler araştırmaya gönüllü olarak katılmıştır. Araştırmaya katılan öğrencilere ait demografik bilgiler Çizelge 3.1'de sunulmuştur.

Çizelge 3.1. Katılımcıların Demografik Bilgileri

Değişkenler	**Seçenek**	**N**	**%**
Cinsiyet	Kadın	1188	47,63
	Erkek	1306	52,37
Eğitim Kademesi	Önlisans	522	20,93

	Lisans	1629	65,32
	Y. Lisans/Doktora	343	13,75
Sınıf Düzeyi	1. Sınıf	707	28,35
	2. Sınıf	827	33,16
	3. Sınıf	435	10,85
	4. Sınıf	525	27,64
İnternette Geçirilen Süre	0-1 Saat	118	4,73
	2-3 saat arası	446	17,89
	4-5 saat arası	838	33,60
	6-7 saat arası	632	25,34
	8 saatten fazla	460	18,44
Aile Gelir Düzeyi	5000 ve altı	425	17,04
	5001-7500	563	22,57
	7501-10000	847	33,96
	10000 üzeri	659	26,43

Çizelge 3.1'deki veriler incelendiğinde; cinsiyet değişkenine göre katılımcıların 1188'i (%47,63) kadın, 1306'sı (%52,37) erkek olduğu; eğitim kademesine göre katılımcıların 522'si ön lisans (%20,93), 1629'u (%65,32) lisans, 343'ünün (%13,75) yüksek lisans/doktora olduğu belirlenmiştir. Sınıf düzeyi değişkenine göre katılımcıların 707'si (%28,35) 1. sınıf, 827'si (%33,16) 2. sınıf, 435'i (%10,85) 3. sınıf, 525'inin ise (%27,64) 4. Sınıf düzeyinde olduğu görülmüştür. İnternette geçirilen süre değişkenine göre katılımcıların 118'i (%4,73) 0-1 saat, 446'sı (%17,89) 2,3 saat, 838'i (%33,60) 4,5 saat, 632'si (%25,34) 6-7 saat, 460'ı ise (%18,44) 8 saatten fazla internette geçirmektedir. Aile gelir düzeyi değişkenine göre ise katılımcıların 425'i (%17,04) 5000 TL ve altı, 563'ü (%22,57) 5001-7500 TL, 847'si (%33,96) 7501-10000 TL, 659'unun da (%26,43) 10000 TL üzeri aile gelir düzeyine sahip oldukları belirlenmiştir.

Çizelge 3.2'de, araştırmaya katılan üniversite öğrencilerinin teknolojik cihaz sahipliği durumunu gösteren veriler yer almaktadır.

Çizelge 3.2. Teknolojik Cihaz Sahipliği Durumu

Akıllı telefon	Dizüstü bilgisayar	Tablet	Masaüstü bilgisayar	Smart tv	Hiçbirini kullanmıyorum	N	%
X						405	16,24
X	**X**					909	36,45

X	**x**		**X**			119	4,77
x	**x**		**X**	**x**		34	1,36
x	**x**			**x**		104	4,17
x	**x**	**x**				223	8,94
x	**x**	**x**	**X**			62	2,48
x	**x**	**x**	**X**	**x**		130	5,21
x	**x**	**x**		**x**		55	2,21
x			**X**			95	3,81
x			**X**	**x**		15	0,60
x				**x**		20	0,80
x		**x**				115	4,61
x		**x**	**X**			23	0,92
x		**x**	**X**	**x**		14	0,56
x		**x**		**x**		8	0,32
	x					19	0,76
	x		**x**			6	0,24
	x		**x**	**x**		3	0,12
	x			**x**		1	0,04
	x	**x**				8	0,32
	x	**x**	**x**			4	0,16
	x	**x**	**x**	**x**		1	0,04
	x	**x**		**x**		3	0,12
			x			22	0,88
			x	**x**		12	0,48
				x		24	0,96
		x				23	0,92
		x	**x**			17	0,68
		x	**x**	**x**		13	0,52
		x		**x**		7	0,28
					Toplam	2494	

Çizelge 3.2'ye göre, öğrencilerin tamamının en az bir teknolojik aracı kullandığı görülmektedir. Öğrencilerin 909'unun (%36,45) ve en yüksek oranla hem akıllı telefon hem dizüstü bilgisayar sahibi olduğu, 1 (%0,04)'inin ise en düşük oranla ile dizüstü bilgisayar, tablet masa üstü bilgisayar ve smart tv sahibi olduğu görülmüştür. Bu veriler, örneklemin araştırma konusu için uygun olduğunun bir göstergesi olarak kabul edilebilir.

3.2. Veri Toplama Araçları

Araştırmada veri toplama amacıyla 3 bölümden oluşan bir form kullanılmıştır. Formun birinci bölümünü araştırmacının hazırladığı kişisel bilgiler soruları, ikinci bölümünü Som-Vural (2016) tarafından geliştirilen Dijital Vatandaşlık Ölçeği, üçüncü bölümünü ise Yılmaz ve diğerleri (2015) tarafından geliştirilen Dijital Veri Güvenliği Farkındalığı Ölçeği oluşturmaktadır.

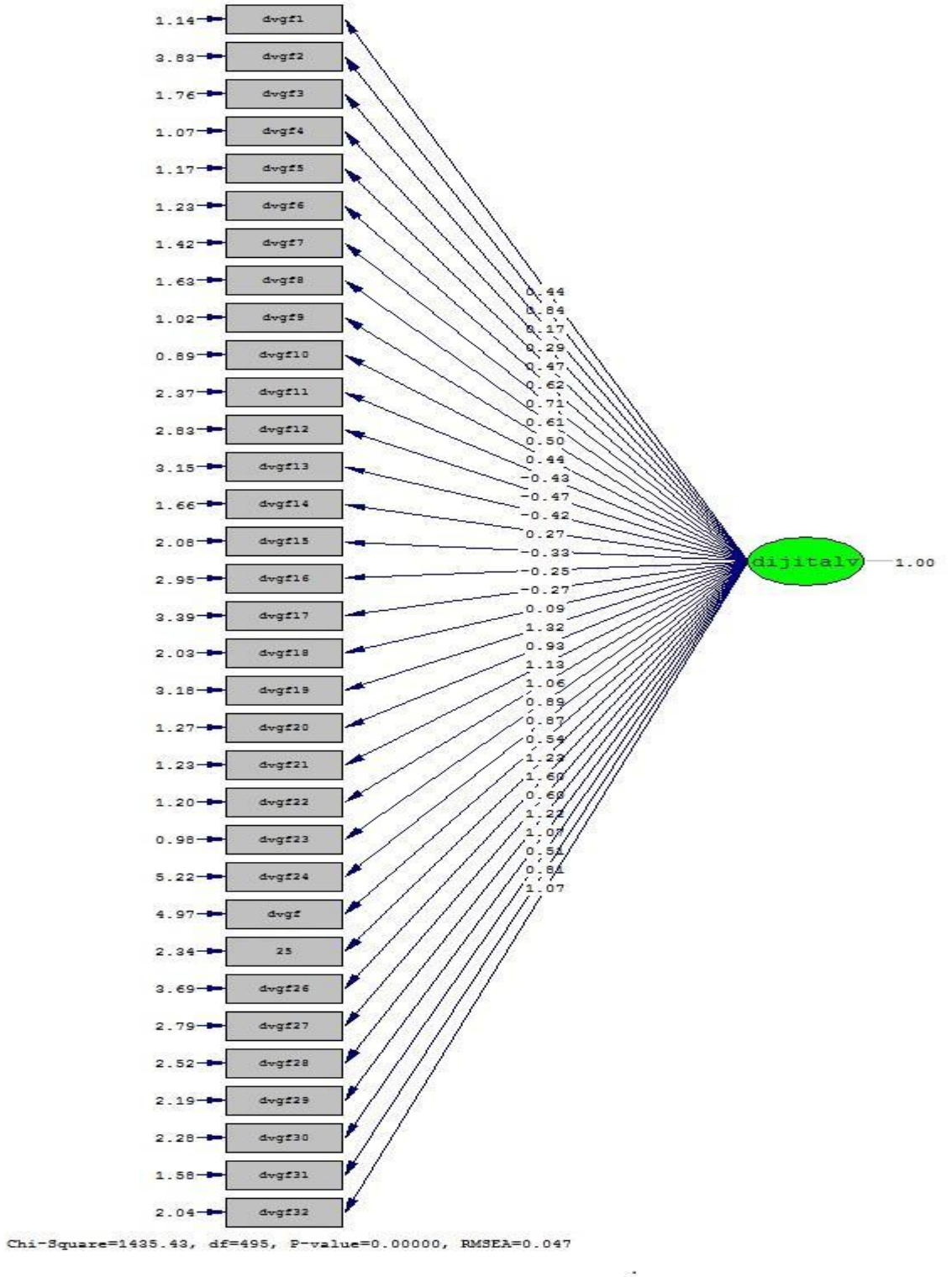
Kişisel Bilgi Soruları: Kişisel bilgi soruları araştırmacı tarafından hazırlanmıştır. Sorularla ilgili öncelikle alan yazın taraması yapılmıştır. Bu şekilde oluşturulan soruların kapsam geçerliliği için 3 BÖTE akademisyeni, 2 BT öğretmeni ve 1 Ölçme Değerlendirme alanı akademisyeninden görüşleri alınmıştır. Görüşler neticesinde güncellenen soruların anlaşılırlığını belirlemek için ise 1 Türkçe öğretmeninden görüşleri alınmış, Türkçe yazım ve imla kurallarına göre düzeltmeler yapılarak sorulara son hali verilmiştir. Formdaki 8 sorunun 6 tanesi demografik bilgi, 2 tanesi ise katılımcıların dijital vatandaşlık ve dijital veri güvenliği farkındalığı görüşlerine ilişkin sorulardır. Form, EK 1' de sunulmuştur.

Dijital Vatandaşlık Ölçeği: Som-Vural (2016) tarafından üniversite öğrencilerinin dijital vatandaşlık düzeyini ölçme amacıyla geliştirilen ölçek 23 madde ve 5 alt faktörden oluşmaktadır. Ölçeğin alt faktörleri çevrimiçi işlemler, doğru kullanım, sağlık, erişim ve toplumsal sorumluluk şeklindedir. Dijital Vatandaşlık Ölçeği'nin geneline ait hesaplanan Cronbach Alfa katsayısı 0,87'dir. Alt faktörlerinin Cronbach Alfa katsayısı ise çevrimiçi işlemler 0,62, doğru kullanım 0,85, sağlık 0,0,68, erişim 0,73, toplumsal sorumluluk 0,63'tür. Yapılan test tekrar test sonucunda ölçeğin hesaplanan güvenirlik korelasyon katsayısı ise 0,70'tir. Ölçek 5'li Likert tipinde olup, (5=Kesinlikle Katılıyorum, 4=Katılıyorum, 3=Kararsızım, 2= Katılmıyorum, 1=Kesinlikle Katılmıyorum) şeklinde seçeneklerden oluşmaktadır. Ölçek maddeleri EK 2'de sunulmuştur. Ölçeğin kullanılmasına ilişkin gerekli izin alınmıştır (EK 3).

Dijital Veri Güvenliği Farkındalığı Ölçeği: Yılmaz, Şahin ve Akbulut (2015) tarafından geliştirilen ölçek 32 sorudan oluşmaktadır. Ölçek maddelerin faktör yükleri ise 0,506 ile 0,689 arasında değişmektedir. Ölçeğin Cronbach Alfa katsayısı 0,945'tir. Ölçekten alınan toplam puanın yüksek olması, dijital veri güvenliği farkındalığının da yüksekliğini göstermektedir. Ölçek 5'li Likert tipinde olup, (1=Kesinlikle Katılıyorum, 2=Katılıyorum, 3=Kararsızım, 4= Katılmıyorum, 5=Kesinlikle Katılmıyorum) şeklinde seçeneklerden oluşmaktadır (EK 4). Ölçeğin kullanılmasına yönelik gerekli izin alınmıştır (EK 5).

Yürütülen bu tez çalışmasında kullanılan Dijital Veri Güvenliği Farkındalık Ölçeği ve Dijital Vatandaşlık Ölçeği için psikometrik özellikler incelenmiştir.

Dijital Veri Güvenliği Farkındalık Ölçeği, öğretmenler için geliştirilmiştir. Bu çalışmada ise öğretmen adayları ile çalışıldığından, öncesinde Doğrulayıcı Faktör Analizi (DFA) yapılarak yapı geçerliği incelenmiştir. DFA'da sınanan modelin yeterliliğini ortaya koymak üzere Ki-Kare Uyum Testi (Chi-Square Goodness), iyilik uyum indeksi (Goodness of Fit Index, GFI), düzeltilmiş iyilik uyum indeksi (Adjustment Goodness of Fit Index, AGFI) karşılaştırmalı uyum indeksi (Comparative Fit Index, CFI), normlaştırılmış uyum indeksi (Normed Fit Index, NFI), normlaştırılmamış uyum indeksi (Non-Normed Fit Index, NNFI), tahmin hatalarının ortalamasının karekökü (Root Mean Square Error of Approximation, RMSEA) ve standartlaştırılmış hata kareleri ortalamasının karekökü (Standardized Root Mean Square Residual, SRMR) incelenmiştir. Yapılan DFA'da elde edilen modelin uyum indeksleri incelenmiş ve minimum ki-kare değerinin ($\chi 2$=1435,43, Sd=495 p=0.00) anlamlı olduğu görülmüştür. Uyum indeksi değerleri ise RMSEA=.047, GFI=.90, AGFI=.89, CFI=.92, NFI=.92, NNFI=.90 ve SRMR=.05 olarak bulunmuştur. İncelenen uyum indekslerine ilişkin mükemmel ve kabul edilebilir uyum ölçütleri, DFA'dan elde edilen tek faktörlü modelin uyumlu olduğunu ve ölçeğin orijinal formundaki faktör yapısının çalışmanın örnekleminde doğrulandığını göstermektedir. Yapılan DFA'ya ait yol diyagramı Şekil 3.1'de verilmiştir.



Şekil 3.1. Doğrulayıcı Faktör Analizi

Çalışmada kullanılan Dijital Veri Güvenliği Farkındalık Ölçeği ve Dijital Vatandaşlık ölçekleri için güvenirlik değeri de incelenmiştir ve elde edilen Cronbach Alpha değerleri sırasıyla .95 ve.93'tür.

3.3. Verilerin Toplanması

Verilerin Trakya Üniversitesi öğrencilerinden toplanması için öncelikle Trakya Üniversitesi Sosyal ve Beşerî Bilimler Araştırmaları Etik Kurulu'ndan onay alınmıştır. Onay belgesi EK 6'da sunulmuştur.

Veriler sınıf ortamında yüz yüze toplanmıştır. Üniversitede dersler öncesi ve dersler sonrası öğrencilere anket uygulaması sağlanmıştır. Uygulama öncesi öğrencilere sözlü olarak tezin konusu ve amacı açıklanmış, katılmak isteyen öğrencilere anket formu dağıtılmıştır.

3.4. Verilerin Analizi

Ölçme araçlarından elde edilen nicel verilerin istatiksel analizi SPSS 25,0 programı ile yapılmıştır. Araştırma kapsamında 2500 üniversite öğrencisine ulaşılmış, ancak anket formunun eksik, hatalı uygulanmasından dolayı veri analizine 2494 öğrenci verisi dahil edilmiştir. Araştırmanın amaçları doğrultusunda elde edilen verilerin frekans ve yüzde dağılımları yapılmıştır. Ölçme araçlarından elde edilen toplam puanların standart sapma, aritmetik ortalama, frekans ve yüzdelik hesaplamaları betimsel istatistikler yardımıyla incelenmiştir. Araştırmada normal dağılım gösteren verilerin analizinde parametrik analiz yöntemlerinden yararlanılmıştır. İkili gruplarda puan ortalamaları karşılaştırılmasında bağımsız örneklem t testi ile ikiden fazla grupların puan ortalamaları karşılaştırmasında tek yönlü ANOVA varyans analizi uygulanmıştır. Ölçek puanlarının karşılaştırılması için Pearson korelasyon analizi yapılmıştır. Açık uçlu soruların analizinde içerik analizi kullanılmıştır.

BÖLÜM 4

BULGULAR

Bu bölümde, tezin araştırma sorularına yanıt bulmak amacıyla gerçekleştirilen analizlere ve bulgulara yer verilmiştir. Elde edilen bulgular, ilgili değişkene ait başlıklar altında sunulmuştur.

4.1. Dijital Veri Güvenliği Farkındalığına Dair Bulgular

Çalışma grubunda yer alan 2500 üniversite öğrencisine dijital veri güvenliği farkındalık ölçeği uygulanmıştır. Bu ölçekten elde edilen veriler doğrultusunda, çalışma grubunun dijital veri güvenliği farkındalıklarına ait betimsel istatistikler Çizelge 4.1'de verilmiştir.

Çizelge 4.1. Çalışma Grubunun Dijital Veri Güvenliği Farkındalıklarına Ait Betimsel İstatistikleri

	Dijital Veri Güvenliği Farkındalığı
Aritmetik Ortalama	127,33
Medyan	129,00
Mod	158
Standart Sapma	20,981
Çarpıklık Katsayısı	-,731
Basıklık Katsayısı	,491

Çizelge 4.1 incelendiğinde dijital veri güvenliği farkındalığı dağılımının sola çarpık (mod>medyan> aritmetik ortalama) ve homojen (V<20) olduğu görülmektedir. Bu durumda çalışma grubunun genelinin dijital veri güvenliği farkındalığının yüksek olduğu yorumu yapılabilir. Dijital veri güvenliği farkındalığı değişkeni için çarpıklık ve basıklık katsayıları incelendiğinde ise bu değerlerin ±1,5 aralığında olduğu görülmüştür. Bu durumda çalışma grubunun dağılımın normal varsayılacağı söylenebilir.

Üniversite öğrencileri ile gerçekleştirilen bu araştırmada katılımcıların dijital veri güvenliği farkındalık durumları cinsiyet, öğrenim görmekte olduğu eğitim kademesi, sınıf düzeyi, günlük ortalama internet kullanma süresi ve ailenin aylık ortalama gelir düzeyi değişkenleri açısından incelenmiştir. Çizelge 4.2'de öğrencilerin dijital veri güvenliği farkındalık puanları arasında cinsiyet açısından fark olup olmadığının incelendiği t testi sonuçları yer almaktadır.

Çizelge 4.2. Dijital Veri Güvenliği Farkındalık Puanlarının Cinsiyete Göre t Testi Sonuçları

Değişken		**N**	$\underline{X}$	**SS**	**Sd**	**t**	**p**
Cinsiyet	**Kadın**	1188	125,29	21,192	2455,434	-4,629	,000
	Erkek	1306	129,18	20,621			

Çizelge 4.2'de yer alan bilgilere göre üniversite öğrencilerinin dijital veri güvenliği farkındalık düzeyleri cinsiyete ($t_{(2455,434)}$ =-4,629 $p<0,05$) göre farklılaşmaktadır. Bu farklılık incelendiğinde erkek öğrencilerin ($\underline{X} = 129,18$) kadınlara ($\bar{X}$=125,29) göre dijital veri güvenliği farkındalık puanlarının daha yüksek olduğu görülmüştür.

Üniversite öğrencilerinin dijital veri güvenliği farkındalık durumları öğrenim görmekte olduğu eğitim kademesi, sınıf düzeyi, günlük ortalama internet kullanma süresi ve ailenin aylık ortalama gelir düzeyi değişkenleri açısından ANOVA analizi ile incelenmiştir.

ANOVA ikiden fazla alt grubu olan değişkenlerin ortalamalar arasındaki farkın istatistiksel olarak anlamlılığını test eden analiz türüdür. Bu bağlamda önce grupların betimsel istatistikleri verilmiştir. Çizelgede alt grupların ortalamaları ve standart sapma değerleri yer almaktadır. Grupların betimsel istatistikler arasındaki küçük ya da büyük farkların istatistiksel olarak anlamlı olup olmadığı devamında yapılan ANOVA ile belirlenmiştir.

Çizelge 4.3'te öğrencilerin dijital veri güvenliği farkındalık puanlarının ilgili değişkenlere ait betimsel istatistikleri yer almaktadır.

Çizelge 4.3. Öğrenim Görmekte Olduğu Eğitim kademesi, Sınıf düzeyi, Günlük Ortalama İnternet Kullanma Süresi ve Ailenin Aylık Ortalama Gelir Düzeyi Değişkenlerine Ait Betimsel İstatistikler

Değişkenler		**N**	$\underline{X}$	**SS**
Eğitim Kademesi	(1) Önlisans	522	125,98	22,177
	(2) Lisans	1629	128,14	20,270
	(3)Y.Lisans/Doktora	343	127,51	22,233
Sınıf Düzeyi	1. Sınıf	707	126,59	21,378
	2. Sınıf	827	126,63	21,311
	3. Sınıf	435	129,33	19,714
	4. Sınıf	525	129,76	20,873
İnternette Geçirilen Süre	(1) 0-1 Saat	118	128,55	20,499
	(2) 2-3 saat arası	446	125,30	21,263
	(3) 4-5 saat arası	838	126,96	20,864
	(4) 6-7 saat arası	632	126,94	20,402
	(5) 8 saatten fazla	460	130,19	21,595
Aile Gelir Düzeyi	(1) 5000 ve altı	425	125,35	22,512
	(2) 5001-7500	563	126,37	20,942
	(3) 7501-10000	847	129,17	20,485
	(4) 10000 üzeri	659	129,61	20,308

Çizelge 4.3 incelendiğinde 2494 katılımcının 522'si ön lisans, 1629'u lisans ve 343'ü yüksek lisans ve doktora seviyesinde öğrenim görmektedir. Eğitim kademesine göre dijital veri güvenliği farkındalık puan ortalamaları incelendiğinde lisans öğrencilerinin ön lisans öğrencilerinden daha yüksek bir ortalamaya, yüksek lisans/doktora öğrencileriyle ise yakın bir ortalamaya sahip olduğu görülmektedir. Sınıf düzeylerine göre dijital veri güvenliği farkındalık ortalamaları incelendiğinde sınıf düzeyi

arttıkça ortalamanın da arttığı ancak bu artışın çok yüksek olmadığı görülmüştür. Veriler internette geçirilen süre bakımından incelendiğinde 118 kişi 1 saatten az, 446 kişi en az 2 en fazla 3 saat, 838 kişi en az 4 en fazla 5 saat, 632 kişi 6-7 saat arası ve 460 kişi 8 saatten fazla zaman geçirdiğini bildirmişlerdir. İnternette geçirilen süreye göre dijital veri güvenliği farkındalığı puan ortalamaları incelendiğinde, internette 1 saatten az ve 8 saatten fazla zaman geçirenlerin diğer kişilere göre farkındalık puan ortalamalarının daha yüksek olduğu gözlenmiştir. Katılımcılardan 425 kişi aile gelir düzeyinin 5000 ve altında olduğunu, 563 kişi 5001 ve 7500 arasında olduğunu, 847 kişi 7501-10000 arasında olduğunu ve 659 kişi 10000 üzerinde olduğunu belirtmişlerdir. Aile gelir düzeyi açısından dijital veri güvenliği farkındalık puanları incelendiğinde gelir düzeyi arttıkça farkındalık puan ortalamasının da arttığı görülmüştür. Bu farklılığın istatistiksel olarak anlamlı olup olmadığı ANOVA ile incelenmiştir. Çizelge 4.4'te katılımcıların dijital veri güvenliği farkındalık puan ortalamalarının eğitim kademesi, sınıf düzeyi, internette geçirilen süre ve aile gelir düzeyine göre farklılık gösterip göstermediğine ilişkin ANOVA sonuçları yer almaktadır.

Çizelge 4.4. Öğrenim Görmekte Olduğu Eğitim Kademesi, Sınıf Düzeyi, Günlük Ortalama İnternet Kullanma Süresi ve Ailenin Aylık Ortalama Gelir Düzeyi Değişkenlerine Ait ANOVA Sonuçları

	Varyansın kaynağı	Kareler toplamı	Sd	Kareler ortalaması	F	p	Anlamlı fark
Eğitim Kademesi	Gruplar arası	3175,152	2	1587,576	3,614	,027	2-1
	Gruplar içi	1094214,555	2491	439,267			
	Toplam	1097389,706	2493				
Sınıf Düzeyi	Gruplar arası	2635,721	3	878,574	1,998	,112	
	Gruplar içi	1094753,985	2490	439,660			
	Toplam	1097389,706	2493				
İnternette	Gruplar arası	5982,916	4	1495,729	3,411	,009	1-2

Geçirilen Süre	Gruplar içi	1091406,791	2489	438,492			2-5
	Toplam	1097389,706	2493				
Aile Gelir Düzeyi	Gruplar arası	9630,952	3	3210,317	7,349	,000	1-3
	Gruplar içi	1087758,755	2490	436,851			1-4
	Toplam	1097389,706	2493				

Çizelge 4.4'te yer alan ANOVA sonuçları incelendiğinde eğitim kademesi değişkenine göre öğrencilerin dijital veri güvenliği farkındalık puan ortalamaları arasındaki farkın istatistiksel olarak anlamlı olduğu sonucuna ulaşılmıştır ($F_{(2,2491)}=3,614$ $p<0,05$). Dijital veri güvenliği farkındalık puan ortalamasının eğitim kademesine göre farklılaşmasının hangi gruplar arasında olduğunu bulmak için Scheffe testi yapılmıştır. Elde edilen sonuçlara göre lisans ve Yüksek lisans/doktora öğrencilerinin farkındalıkları ön lisans öğrencilerinden daha yüksek olduğu görülmüştür, lisans ve yüksek lisans/doktora öğrencileri arasında ise fark bulunmamıştır. Sınıf düzeyine göre öğrencilerin dijital veri güvenlik farkındalığı puan ortalamaları arasındaki farkın istatistiksel olarak anlamlı olmadığı sonucuna ulaşılmıştır ($F_{(3,2490)}=1,998$ $p>0,05$). Çizelge 4.4 incelendiğinde, üniversite öğrencilerin dijital veri güvenliği farkındalık puan ortalamaları arasında internette geçirilen süreye göre istatistiksel olarak anlamlı bir fark olduğu görülmüştür ($F_{(4,2489)}=3,411$ $p<0,05$). Dijital veri güvenliği farkındalık puan ortalamasının internette geçirilen süreye göre farklılaşmasının hangi gruplar arasında olduğunu bulmak için Scheffe testi yapılmıştır. Elde edilen sonuçlara göre; internette 0-1 saat arası zaman geçiren kişilerin 2-3 saat zaman geçirenlere göre farkındalıklarının daha yüksek olduğu, benzer şekilde internette 8 saatten fazla zaman geçiren öğrencilerin 2-3 saat zaman geçirenlerle arasında istatistiksel olarak anlamlı bir fark olduğu ve 8 saatten fazla zaman geçirenlerin dijital veri güvenliği farkındalık puanlarının diğerlerine göre daha yüksek olduğu görülmüştür. İnternette 2-3 saat arasında zaman geçirenler ile 4-5 saat arası ve 6-7 saat arası zaman geçirenler arasında ise dijital veri güvenliği farkındalık puanları açısından anlamlı farklılık bulunmamıştır. Çizelge 4.4'te yer alan aile

gelir düzeyi değişkenine ait ANOVA sonucu incelendiğinde dijital veri güvenliği farkındalık durumlarının aile gelir düzeyine göre istatistiksel olarak anlamlı farklılık ($F_{(3,2490)} = 7{,}349$ $p<0{,}05$) gösterdiği görülmektedir. Dijital veri güvenliği farkındalık puan ortalamasının aile gelir düzeyine göre farklılaşmasının hangi gelir düzeyleri arasında olduğunu bulmak için Scheffe testi yapılmıştır. Elde edilen sonuçlara göre; aile gelir düzeyi 5000 ve altında olan öğrencilerin farkındalık düzeyleri aile gelir düzeyi 7500 ve 1000 arasında ve 10000 üzerinde olanlara göre daha düşük olduğu görülmüştür. Buna göre aile gelir düzeyi arttıkça dijital veri güvenliği farkındalığının da arttığı söylenebilir.

Çalışma kapsamında katılımcılara dijital veri güvenliği konusunda farkındalığın ve bilgi düzeyinin artırılmasıyla ilgili olarak üniversite yönetiminden beklentilerinin neler olduğu sorulmuştur. 1395 öğrenci soruya yanıt vermiştir. Verilen yanıtlar incelendiğinde öğrenciler bu dijital veri güvenliği konusunda bilgilerinin kısıtlı olduğu ve beklentilerinin de ders, seminer ya da konferans ile bilgilendirme olduğu görülmüştür. 1395 katılımcından 956'sı (%68) ilgili konunun derslerde işlenmesinin iyi olacağını, 439'u (%32) üniversitedeki hocaların bu konuyla ilgili seminer ya da konferans vermemesinin bilgilendirme açısından faydalı olacağı görüşünü bildirmişlerdir.

4.2. Dijital Vatandaşlığa Dair Bulgular

Çalışma grubunda yer alan 2494 üniversite öğrencisine dijital vatandaşlık ölçeği uygulanmıştır. Bu ölçekten elde edilen veriler doğrultusunda çalışma grubunun dijital vatandaşlık düzeylerine ait betimsel istatistikler Çizelge 4.5'te verilmiştir.

Çizelge 4.5. Çalışma Grubunun Dijital Vatandaşlık Puanlarına Ait Betimsel İstatistikleri

	Dijital Veri Güvenliği Farkındalığı
Aritmetik Ortalama	94,31
Medyan	96,00
Mod	115
Standart Sapma	15,366
Çarpıklık Katsayısı	-,986
Basıklık Katsayısı	,443

Çizelge 4.5 incelendiğinde; dijital vatandaşlık dağılımının sola çarpık (mod>medyan> aritmetik ortalama) ve homojen (V<20) olduğu görülmektedir. Bu durumda çalışma grubunun genelinin dijital vatandaşlık düzeyinin yüksek olduğu yorumu yapılabilir. Dijital vatandaşlık değişkeni için çarpıklık ve basıklık katsayıları

incelendiğinde ise bu değerlerin ±1,5 aralığında olduğu görülmüştür. Bu durumda çalışma grubunun dağılımın normal varsayılacağı söylenebilir.

Üniversite öğrencileri ile gerçekleştirilen bu araştırmada; katılımcıların dijital vatandaşlık durumları cinsiyet, öğrenim görmekte olduğu eğitim kademesi, sınıf düzeyi, günlük ortalama internet kullanma süresi ve ailenin aylık ortalama gelir düzeyi değişkenlerine değişkenleri açısından incelenmiştir. Çizelge 4.6'da öğrencilerin dijital vatandaşlık düzeylerinde cinsiyet açısından fark olup olmamasının incelendiği t testi sonuçları yer almaktadır.

Çizelge 4.6. Dijital Vatandaşlık Puanlarının Cinsiyete Göre t Testi Sonuçları

Değişken		**N**	$\underline{X}$	**SS**	**Sd**	**t**	**p**
Cinsiyet	**Kadın**	1188	93,31	15,464	2492	-3,088	,002
	Erkek	1306	95,21	15,227			

Çizelge 4.6'da yer alan bilgilere göre üniversite öğrencilerinin dijital vatandaşlık düzeyleri cinsiyete ($t_{(2492)}$ =-3,088 $p<0,05$) göre farklılaşmaktadır. Bu farklılık incelendiğinde erkek öğrencilerin ($\underline{X} = 95,21$) kadınlara ($\bar{X}$=93,31) göre dijital vatandaşlık puanlarının daha yüksek olduğu görülmüştür.

Üniversite öğrencilerinin dijital vatandaşlık durumları öğrenim görmekte olduğu eğitim kademesi, sınıf düzeyi, günlük ortalama internet kullanma süresi ve ailenin aylık ortalama gelir düzeyi değişkenleri açısından ANOVA analizi ile incelenmiştir. Çizelge 4.7'de öğrencilerin bu değişkenlere ait betimsel istatistikleri yer almaktadır.

Çizelge 4.7. Öğrenim Görmekte Olduğu Eğitim Kademesi, Sınıf Düzeyi, Günlük Ortalama İnternet Kullanma Süresi ve Ailenin Aylık Ortalama Gelir Düzeyi Değişkenlerine Ait Betimsel İstatistikler

Değişkenler		**N**	$\underline{X}$	**SS**
Eğitim Kademesi	(1) Önlisans	522	92,68	16,683
	(2) Lisans	1629	95,05	14,816
	(3)Y.Lisans/Doktora	343	94,24	15,633

Sınıf Düzeyi	1. Sınıf	707	93,25	16,042
	2. Sınıf	827	94,10	15,178
	3. Sınıf	435	94,62	13,602
	4. Sınıf	525	96,13	15,944
İnternette Geçirilen Süre	(1) 0-1 Saat	118	96,42	16,700
	(2) 2-3 saat arası	446	93,98	14,905
	(3) 4-5 saat arası	838	94,00	15,850
	(4) 6-7 saat arası	632	93,54	14,802
	(5) 8 saatten fazla	460	95,69	15,249
Aile Gelir Düzeyi	(1) 5000 ve altı	425	93,51	17,770
	(2) 5001-7500	563	94,19	15,118
	(3) 7501-10000	847	95,16	14,579
	(4) 10000 üzeri	659	95,19	14,812

Çizelge 4.7 incelendiğinde; 2494 katılımcının 522'si ön lisans, 1629'u lisans ve 343'ü yüksek lisans ve doktora seviyesinde öğrenim görmektedir. Eğitim kademesine göre dijital vatandaşlık puan ortalamaları incelendiğinde lisans öğrencilerinin ön lisans öğrencilerinden daha yüksek bir ortalamaya, yüksek lisans/doktora öğrencileriyle ise yakın bir ortalamaya sahip olduğu görülmektedir. Sınıf düzeylerine göre dijital vatandaşlık ortalamaları incelendiğinde sınıf düzeyi arttıkça ortalamanın da arttığı görülmüştür. Veriler internette geçirilen süre bakımından incelendiğinde 118 kişi 1 saatten az, 446 kişi en az 2 en fazla 3 saat, 838 kişi en az 4 en fazla 5 saat, 632 kişi 6-7 saat arası ve 460 kişi 8 saatten fazla zaman geçirdiğini bildirmişlerdir. İnternette geçirilen süreye göre dijital vatandaşlık puan ortalamaları incelendiğinde internette çok az ve çok fazla zaman geçirenlerin diğer kişilere göre vatandaşlık puan ortalamalarının daha yüksek olduğu gözlenmiştir. Katılımcılardan 425 kişi aile gelir düzeyinin 5000 ve altında olduğunu, 563 kişi 5001 ve 7500 arasında olduğunu, 847 kişi 7501-10000 arasında olduğunu ve 659 kişi 10000 üzerinde olduğunu belirtmişlerdir. Aile gelir düzeyi açısından dijital vatandaşlık puanları incelendiğinde gelir düzeyi arttıkça vatandaşlık puan

ortalamasının da arttığı görülmüştür. Bu farklılığın istatistiksel olarak anlamlı olup olmadığı ANOVA ile incelenmiştir.

Çizelge 4.8'de katılımcıların dijital vatandaşlık puan ortalamalarının eğitim kademesi, sınıf düzeyi, internette geçirilen süre ve aile gelir düzeyine göre farklılık gösterip göstermediğine ilişkin ANOVA sonuçları yer almaktadır.

Çizelge 4.8. Öğrenim Görmekte Olduğu Eğitim Kademesi, Sınıf Düzeyi, Günlük Ortalama İnternet Kullanma Süresi ve Ailenin Aylık Ortalama Gelir Düzeyi Değişkenlerine Ait ANOVA Sonuçları

	Varyansın kaynağı	**Kareler toplamı**	**Sd**	**Kareler ortalaması**	**F**	**p**	**Anlamlı fark**
Eğitim Kademesi	Gruplar arası	2681,807	2	1340,903	5,700	,003	1-2
	Gruplar içi	585983,766	2491	235,240			
	Toplam	588665,572	2493				
Sınıf Düzeyi	Gruplar arası	3172,545	3	1057,515	4,497	,004	1-4
	Gruplar içi	585493,027	2490	235,138			2-4
	Toplam	588665,572	2493				
İnternette Geçirilen Süre	Gruplar arası	1902,937	4	475,734	3,018	,039	1-2
	Gruplar içi	586762,635	2489	235,742			2-5
	Toplam	588665,572	2493				
Aile Gelir Düzeyi	Gruplar arası	2147,046	3	715,682	3,038	,028	1-3
	Gruplar içi	586518,526	2490	235,550			1-4

	Toplam	588665,572	2493				

Çizelge 4.8'de yer alan ANOVA sonuçları incelendiğinde eğitim kademesi değişkenine göre öğrencilerin dijital vatandaşlık puan ortalamaları arasındaki farkın istatistiksel olarak anlamlı olduğu sonucuna ulaşılmıştır ($F_{(2,2491)} = 5,700$ $p<0,05$). Dijital vatandaşlık puan ortalamasının eğitim kademesine göre farklılaşmasının hangi gruplar arasında olduğunu bulmak için Scheffe testi yapılmıştır. Elde edilen sonuçlara göre lisans ve yüksek lisans/doktora öğrencilerinin vatandaşlık puanlarının ön lisans öğrencilerinden daha yüksek olduğu görülmüştür. Lisans ve yüksek lisans/doktora öğrencileri arasında ise fark bulunmamıştır. Katılımcıların sınıf düzeyine göre dijital vatandaşlık puan ortalamaları arasında fark olup olmadığı incelendiğinde, bir fark olduğu ve bu farkın istatistiksel olarak anlamlı olduğu sonucuna ulaşılmıştır ($F_{(3,2490)} = 4,497$ $p<0,05$). Yapılan Scheffe testi sonucunda dördüncü sınıfların birinci ve ikinci sınıflara göre dijital vatandaşlık puanlarının daha yüksek olduğu, sınıf düzeyi arttıkça dijital vatandaşlık düzeyinin de arttığı görülmüştür. Çizelge 4.8 incelendiğinde üniversite öğrencilerin dijital vatandaşlık puan ortalamaları arasında internette geçirilen süreye göre istatistiksel olarak anlamlı bir fark olduğu görülmüştür ($F_{(4,2489)} = 3,018$ $p<0,05$). Dijital vatandaşlık puan ortalamasının internette geçirilen süreye göre farklılaşmasının hangi gruplar arasında olduğunu bulmak için Scheffe testi yapılmıştır. Elde edilen sonuçlara göre; internette 0-1 saat arası zaman geçiren kişilerin 2-3 saat zaman geçirenlere göre dijital vatandaşlık eğilimlerinin daha yüksek olduğu, benzer şekilde internette 8 saatten fazla zaman geçiren öğrencilerin 2-3 saat zaman geçirenlerle arasında istatistiksel olarak anlamlı bir fark olduğu ve 8 saatten fazla zaman geçirenlerin dijital vatandaşlık puanlarının diğerlerine göre daha yüksek olduğu görülmüştür. İnternette 2-3 saat arasında zaman geçirenler ile 4-5 saat arası ve 6-7 saat arası zaman geçirenler arasında ise dijital vatandaşlık puanları açısından anlamlı farklılık bulunmamıştır. Çizelge 4.8'de yer alan aile gelir düzeyi değişkenine ait ANOVA sonucu incelendiğinde; dijital vatandaşlık durumlarının aile gelir düzeyine göre istatistiksel olarak anlamlı farklılık ($F_{(3,2490)} = 3,038$ $p<0,05$) gösterdiği görülmektedir. Dijital vatandaşlık puan ortalamasının aile gelir düzeyine göre farklılaşmasının hangi gelir düzeyleri arasında olduğunu bulmak için Scheffe testi yapılmıştır. Elde edilen sonuçlara göre aile gelir düzeyi 5000 ve altında olan öğrencilerin

dijital vatandaşlık eğilimleri aile gelir düzeyi 7500 ve 1000 arasında ve 10000 üzerinde olanlara göre daha düşük olduğu görülmüştür. Buna göre aile gelir düzeyi arttıkça dijital vatandaşlık eğiliminin de arttığı söylenebilir.

Çalışma kapsamında katılımcılara dijital vatandaşlık konusunda farkındalığın ve bilgi düzeyinin artırılmasıyla ilgili olarak üniversite yönetiminden beklentilerinin neler olduğu sorulmuştur. 1265 öğrenci soruya yanıt vermiştir. Verilen yanıtlar incelendiğinde; öğrencilerin dijital vatandaşlık konusunda bilgileri kısıtlıdır ve beklentileri ders, seminer ya da konferans ile bilgilendirme yapılması yönündedir. 1265 katılımcından 872'si (%69) ilgili konunun derslerde işlenmesinin iyi olacağını, 403'ü (%31) üniversitedeki hocaların bu konuyla ilgili seminer ya da konferans vermemesinin bilgilendirme açısından faydalı olacağı görüşünü bildirmişlerdir.

4.3. Dijital Veri Güvenliği Farkındalığı ve Dijital Vatandaşlık Arasındaki İlişkiye Dair Bulgular

Araştırmanın temel problemlerinden biri de üniversite öğrencilerinin dijital veri güvenliği farkındalıkları ile dijital vatandaşlık arasındaki ilişkinin incelenmesidir. Bu amaç doğrultusunda 2500 üniversite öğrencisinden elde edilen veriler incelenmiş ve normal dağılım gösteren dijital veri güvenliği farkındalık puanları ve dijital vatandaşlık puanları arasında ilişki Pearson korelasyon katsayısı ile incelenmiştir.

Çizelge 4.9. Dijital Vatandaşlık ve Dijital Veri Güvenliği Farkındalığı İlişkisi

	Dijital Vatandaşlık
Dijital Veri güvenliği Farkındalığı	0,759*

* $p<0,05$

Elde edilen bulgulara göre Çizelge 4.9'da yer aldığı üzere dijital veri güvenliği farkındalığı ve dijital vatandaşlık arasında yüksek düzeyde pozitif bir ilişki (r=0,759**) bulunmuştur ve bu ilişki istatistiksel olarak anlamlıdır($p<0,05$). Elde edilen korelasyon değerinin determinasyon katsayısı incelendiğinde (0,58), bu iki değişkenin birbirini etkileme yüzdesinin %58 olduğu söylenebilir.

BÖLÜM 5

TARTIŞMA

Bu bölümde, araştırmada elde edilen bulgular doğrultusunda daha önce yapılmış çalışmaların sonuçları araştırma soruları kapsamında tartışılmıştır.

"Üniversite öğrencilerinin dijital vatandaşlık düzeyleri nedir?"

Çalışmadan elde edilen bulgulara göre; katılımcıların genelinin dijital vatandaşlık düzeyinin yüksek olduğu görülmüştür. Çalışmanın sonuçlarının öğretmen adaylarının dijital vatandaşlık düzeylerinin değerlendirildiği Kocadağ (2012) çalışması ve Sosyal Bilgiler öğretmen adaylarının bazı değişkenler bakımından dijital vatandaşlık davranışlarının incelendiği Aslan (2016) çalışması ile benzer olduğu görülmektedir. Aynı şekilde sınıf öğretmenleri adaylarının dijital vatandaşlık düzeyleri ve siber zorbalık eğilimlerinin arasındaki ilişkinin incelendiği Sakallı (2015) çalışması ve sınıf öğretmeni adaylarının dijital vatandaşlık düzeylerinin dijital vatandaşlık alt boyutlarına göre incelendiği Bakır (2016)'ın çalışmasının bulguları da mevcut tez çalışması ile benzerdir. Sosyal Bilgiler öğretmenlerinin dijital vatandaşlık düzeylerinin incelendiği Aygün (2019) tarafından yürütülen çalışmanın bulgularının da benzerlik gösterdiği belirlenmiştir. Bu çalışmalarda da katılımcıların dijital vatandaşlık düzeyleri yüksek olarak saptanmıştır. Lindsey (2015)'in çalışmasında ise katılımcıların dijital vatandaşlık düzeyleri başlangıçta yaptıkları taramada düşük olarak bulmuşlardır. Ancak tez çalışmasında uyguladıkları strateji sonrasında dijital vatandaşlık düzeylerini yüksek olarak bildirmişlerdir. Çalışmanın sonuçları ile farklılık gösteren çalışmalara da rastlanmıştır. Öğretmen adaylarının dijital vatandaşlık düzeylerini inceleyen Prensky (2005), katılımcıların dijital vatandaşlık düzeylerini düşük bildirmiştir. Çalışmasında öğrencilerin öğretmenlerden

daha farklı olduklarını, öğretmenlerin günümüzde dijital yerli olarak nitelendirilen öğrencilere yeterli düzeyde rehberlik yapamadıklarını vurgulamaktadır. Benzer şekilde Kilci (2019)'nin sosyal bilgiler öğretmenleri ile gerçekleştirdiği çalışmada da öğretmenlerin dijital vatandaşlık düzeylerinin zayıf olduğu belirlenmiştir. Mevcut tez çalışmasında katılımcıların dijital vatandaşlık düzeylerinin yüksek olması, sahip oldukları teknolojik cihaz sahipliğine ve internette geçirdikleri sürenin yüksek olmasına bağlanabilir. Çünkü katılımcılar en az bir teknolojik cihaza sahip olup, en yüksek oranla (%36,45) hem akıllı telefon hem dizüstü bilgisayar sahibi olduğu görülmüştür. Bunun yanı sıra dijital vatandaşlık konusunda Türkiye'deki bilinçlendirme çalışmalarının süreç içerisinde artmasının da bunda etkili olduğu düşünülmektedir.

"Üniversite öğrencilerinin dijital veri güvenliği farkındalığı hangi düzeydedir?"

Çalışmadan elde edilen bulgulara göre; katılımcıların genelinin dijital veri güvenliği farkındalığının yüksek olduğu görülmüştür. Ortaöğretim öğrencilerinin dijital okuryazarlık ve bilgi güvenliği düzeylerinin ölçüldüğü Talan ve Aktürk (2021) çalışması, üniversite öğrencilerinin dijital okuryazarlık düzeyleri ile dijital veri güvenliği farkındalık düzeyleri arasındaki ilişkinin incelendiği Göldağ (2021) çalışmasının bulguları mevcut tez çalışması ile benzerlik göstermektedir. Aynı şekilde öğretmenlerin dijital veri güvenliği farkındalığının incelendiği Yılmaz ve arkadaşları (2016) tarafından yürütülen çalışmanın sonuçları da bu bulgularla paralellik göstermektedir. Benzer şekilde meslek yüksekokulu öğrencilerinin bilgi güvenliği farkındalık düzeylerinin incelendiği Sağır ve arkadaşlarının (2018) çalışması ve eğitim fakültesi öğrencileri ile diğer fakültelerdeki öğrencilerin siber güvenlik farkındalıklarının karşılaştırıldığı Semerci (2019) çalışmasının bulguları da benzerdir. Öğretmen adaylarının sayısal yetkinlik düzeylerinin belirlenmesi amacıyla yürütülen Timur, Timur ve Akkoyunlu (2014)'nun çalışmalarında dijital veri güvenliği farkındalığı düzeyleri orta düzey olarak belirlenmiştir. Spor bilimleri fakültesi öğrencilerinin bireysel yenilikçilik düzeylerinin dijital okuryazarlığa etkisinin yapısal eşitlik modeli ile incelendiği Güngör ve Kurtipek (2020) tarafından yapılmış çalışmada da bu araştırma bulgusundan farklı olarak katılımcıların dijital veri güvenliği farkındalığı düzeyleri orta düzey olarak tespit edilmiştir. Tekerek ve Tekerek (2013) tarafından yapılan ilköğretim ve lise öğrencileri ile yürütülen çalışmada katılımcıların bilgisayar ve bilgi güvenliği farkındalık düzeyleri incelendiği çalışmada da mevcut çalışmadan farklı olarak katılımcıların dijital veri güvenliği farklılığı düzeyi düşük olarak

bildirilmiştir. Alan yazında ulaştığımız çalışmalardaki farklılığın, araştırmalara dahil edilen katılımcıların sahip oldukları teknolojik cihaz türü ve sayısına, araştırmanın mevcut çalışmadan daha önce yapılmasına ve farklı öğretim kademelerinde olmasından kaynaklanabileceği düşünülmektedir. Mevcut çalışmada katılımcıların genelinin dijital veri güvenliği farkındalık düzeylerinin yüksek çıkmasının temel nedeni ise, çalışmanın diğer araştırmaların yapıldığı yıldan daha sonra yapılmasına yorumlanabilir. Çünkü teknolojinin gelişmesi, internetin yaşamın her alanında kullanılabilir hale gelmesi gibi nedenler, dijital veri güvenliği farkındalığını daha ön plana çıkarmaktadır. Ayrıca eğitim düzeylerinin diğer araştırma örnekleminin eğitim kademesinden yüksek olması ve katılımcıların dijital vatandaşlık düzeylerinin de yüksek olmasında etken olduğu düşünülmektedir.

"Üniversite öğrencilerinin dijital veri güvenliği farkındalıkları ile dijital vatandaşlık düzeyleri arasında istatistiksel olarak anlamlı bir ilişki var mıdır?"

Çalışmadan elde edilen bulgulara göre; katılımcıların dijital veri güvenliği farkındalığı ve dijital vatandaşlık düzeyleri arasında yüksek oranda pozitif bir ilişki (r=0,759**) olduğu bulunmuştur ve bu ilişkinin istatistiksel olarak anlamlı olduğu saptanmıştır. Talan ve Aktürk (2021) tarafından lise öğrencilerinde dijital bilgi güvenliği farkındalık ve dijital okuryazarlık düzeylerinin incelendiği çalışmada dijital veri güvenliği farkındalığı ile dijital okuryazarlık arasında pozitif yönlü anlamlı bir ilişki olduğu saptanmıştır. Bu durum iki değişkenin birlikte arttığı veya azaldığı yönünde yorumlanabilir. Bu çalışmanın lise öğrencileri düzeyinde yapılmış olmasına rağmen bulgularının mevcut çalışma ile paralellik gösterdiği görülmektedir. Alan yazında iki değişkenin aynı anda kullanıldığı çalışmaların sınırlı olduğu görülmektedir. Ancak günümüzde teknolojide yaşanan gelişmelere paralel olarak, sosyal medya uygulamalarının yaygınlaşması ve hemen her işin internet tabanlı uygulamalar üzerinden yapılabilir duruma gelmesinden dolayı, ilgili alanda bundan sonra yapılacak çalışmaların bu değişkenler üzerinde yoğunlaşabileceği düşünülmektedir.

"Üniversite öğrencilerinin dijital veri güvenliği farkındalıkları; cinsiyet, öğrenim görmekte olduğu eğitim kademesi, sınıf, günlük ortalama internet kullanma süresi, teknolojik cihaz sahipliği, ailenin aylık ortalama gelir düzeyi değişkenlerine göre farklılık göstermekte midir?"

Cinsiyet Değişkenine Göre;

Üniversite öğrencilerinin dijital veri güvenliği farkındalık düzeyleri cinsiyete göre farklılaşmaktadır. Bu farklılık incelendiğinde erkek öğrencilerin kadınlara göre dijital veri güvenliği farkındalık puanlarının daha yüksek olduğu görülmüştür. Yılmaz ve arkadaşları (2016) tarafından yürütülen lise öğrencilerinde dijital bilgi güvenliği farkındalık ve dijital okuryazarlık düzeylerinin incelendiği çalışma ve dijital veri güvenliği farkındalığı ile dijital okuryazarlık arasındaki ilişkinin incelendiği Talan ve Aktürk (2021) çalışmasının bulguları benzer niteliktedir. Solmaz (2020); üniversite öğrencilerinin bilgi güvenliği farkındalığını etkileyen etmenleri ele alan Farooq ve arkadaşları (2015)'nın çalışması ve Göldağ (2021) tarafından üniversite öğrencilerinin dijital okuryazarlık düzeyleri ile dijital veri güvenliği farkındalık düzeylerinin arasındaki ilişkinin incelendiği çalışmaların cinsiyet değişkenine bağlı sonuçları, mevcut tez çalışmasını destekler niteliktedir. Üniversite öğrencilerinin mobil güvenlik farkındalığı ve dijital veri güvenliği farkındalıklarının belirlenmesi amacıyla Bıkmaz (2017) tarafından yapılmış çalışmanın; Mart (2012) ve üniversite öğrencilerinin bilgi güvenliği ile bilgi farkındalığının incelendiği Arıtürk (2015)'ün çalışmasının bulguları mevcut çalışma ile çelişmektedir. Benzer şekilde, dijital veri güvenliği farkındalığı ölçeğinin geliştirilmesi amacıyla Yılmaz ve arkadaşları (2015) tarafından yapılan çalışma ve üniversitelerde bilgi işlem daire başkanlığı çalışanlarında siber güvenlik ve dijital veri güvenliği farkındalıklarının belirlenmesini amaçlayan Gündüzalp (2021)'ın çalışmasının bulguları da çelişmektedir. Bilgi güvenliği farkındalığının bireysel özellikler çerçevesinde incelendiği McCormac ve arkadaşları (2017) tarafından yürütülen araştırmanın cinsiyet değişkenine bağlı sonuçlarının da bu tez çalışmasının sonuçları ile çeliştiği görülmektedir. Bu çalışmalarda, kadınların dijital veri güvenliği farkındalıklarının erkeklere nazaran daha yüksek olduğu bildirilmiştir. Bu farklılığın nedeni olarak kadınların dijital ortamlardaki tehlikelerden erkeklere göre daha fazla bilgi sahibi oldukları düşünülmektedir. Akça ve Kaya (2016) tarafından yapılmış çalışmada da günümüzde internet teknolojilerinin kullanımı, toplumsal gelenek ve göreneklerden dolayı kadınların erkeklere nazaran daha dezavantajlı konumda oldukları bildirilmektedir. Aynı çalışmada kadınlar ve erkekler arasındaki internet teknolojileri kullanımının toplumların sosyoekonomik durumlarına göre farklılık gösterdiği belirlenmiştir. Kadınlarda eğitim düzeyi arttıkça, internet ve bilgisayar kullanımının da

daha fazla olduğu görülmüştür. Bu bağlamda kadınların dijital ortamlarda kendilerini güvende hissedebilmeleri için daha bilinçli olmaya çalıştıkları düşünülebilir. Bu tez çalışmasının bulgularına göre, erkek öğrencilerin ($\underline{X} = 129{,}18$) kadınlara (X=125,29) göre dijital veri güvenliği farkındalık puanlarının daha yüksek olmaları ise; erkek öğrencilerin sayısının fazla olmasına, erkeklerin dijital veri güvenliğine daha fazla önem vermesine ve Akça ve Kaya (2016), Dixon ve arkadaşları (2014) tarafından yapılmış çalışmaların bulgularından da anlaşıldığı üzere, günümüz toplumunda kadınların toplumsal cinsiyet bakımından bilinç düzeylerinin yeteri kadar yüksek olmamasına bağlanabilir.

Öğrenim görmekte olduğu eğitim kademesi değişkenine göre;

Eğitim kademesine göre dijital veri güvenliği farkındalık puan ortalamaları incelendiğinde lisans öğrencilerinin ön lisans öğrencilerinden daha yüksek bir ortalamaya, yüksek lisans/doktora öğrencileriyle ise yakın bir ortalamaya sahip olduğu görülmektedir. Eğitim kademesi değişkenine göre öğrencilerin dijital veri güvenliği farkındalık puan ortalamaları arasındaki farkın istatistiksel olarak anlamlı olduğu sonucuna ulaşılmıştır. Lisans ve yüksek lisans/doktora öğrencilerinin farkındalıklarının ön lisans öğrencilerinden daha yüksek olduğu görülmüştür, lisans ve yüksek lisans/doktora öğrencileri arasında ise fark bulunmamıştır. Yılmaz ve arkadaşları (2016); üniversitelerde bilgi işlem daire başkanlığı çalışanlarında siber güvenlik ve dijital veri güvenliği farkındalıklarının belirlenmesi için Gündüzalp (2021) tarafından yapılmış çalışmaların sonuçları da bu tez çalışmasını desteklemektedir. Çalışmada katılımcıların öğrenim kademesi değişkenine göre dijital veri güvenliği farkındalık puan ortalamaları arasında anlamlı farklılık olduğu bildirilmiştir. Alan yazında üniversite öğrencilerinin katılımı ile yürütülen ve dijital okuryazarlık düzeyleri ile dijital veri güvenliği farkındalık düzeylerinin arasındaki ilişkinin incelendiği Göldağ (2021)'ın çalışmasının, Farooq ve arkadaşları (2015) tarafından yapılan üniversite öğrencilerinin bilgi güvenliği farkındalığını etkileyen etmenleri ele alan çalışmaların, öğrenim kademesi değişkenine bağlı sonuçları mevcut tez çalışmasında farklılık göstermektedir. Mevcut tez çalışmasında eğitim kademesi değişkenine göre katılımcıların dijital veri güvenliği farkındalık puan ortalamaları arasında anlamlı farklılığın olmadığı saptanmıştır. Bu tez çalışmasındaki katılımcıların öğretim kademelerinin ve sınıf düzeylerinin farklı olması, eğitim kademelerinde okutulan derslerin farklı olması, çalışmalardan elde edilen sonuçlar

üzerinde etkili olabileceği söylenebilir. Ayrıca, araştırmalarda dijital veri güvenliği farkındalıklarını ölçmek amacıyla uygulanan veri toplama araçlarının birbirinden farklı olmasının sonuçları farklılaştırabileceği düşünülebilir.

Sınıf düzeyi değişkenine göre;

Sınıf düzeylerine göre dijital veri güvenliği farkındalık ortalamaları incelendiğinde, sınıf düzeyi arttıkça ortalamanın da arttığı, ancak bu artışın çok yüksek olmadığı görülmüştür. Sınıf düzeyine göre öğrencilerin dijital veri güvenlik farkındalığı puan ortalamaları arasındaki farkın istatistiksel olarak anlamlı olmadığı sonucuna ulaşılmıştır. Bu durum öğrencilerin sınıf düzeyine uygun şekilde dijital veri güvenliği ile ilişkin bir ders okumamalarına ve bu konuda bilgilendirilmemelerine bağlanabilir. Öğrencilerin sınıf düzeyine uygun olarak dijital veri güvenliği hakkında bilgilendirilmeleri farkındalık düzeylerini arttırmada etkili olabileceği yönünde yorumlanabilir. Ortaöğretim öğrencilerinin dijital okuryazarlık ve bilgi güvenliği düzeylerinin ölçüldüğü Talan ve Aktürk (2021)'ün çalışmasının bulguları mevcut çalışma ile benzerdir. Benzer şekilde öğretmen adaylarının siber bilgi güvenliği farkındalıkları ve dijital vatandaşlık düzeylerinin değişkenlere göre incelendiği Solmaz (2020)'ın çalışması ve öğretmenlerin dijital veri güvenliği farkındalığının incelendiği Yılmaz ve arkadaşları (2016) tarafından yürütülen çalışmaların sonuçları da benzerdir. Bu benzerliği; araştırmalardaki çalışma grubunun cinsiyet, aile gelir düzeyi, öğrenim kademesi, sınıf düzeyi gibi demografik özelliklerinin, araştırmaların yapıldıkları yılların birbirine yakın olmasına dayandırmak mümkündür.

İnternette geçirilen süre değişkenine göre;

Üniversite öğrencilerin dijital veri güvenliği farkındalık puan ortalamaları arasında internette geçirilen süreye göre istatistiksel olarak anlamlı bir farklılık olduğu görülmüştür. Farklılığın; internette 0-1 saat arası zaman geçiren kişilerin 2-3 saat zaman geçirenlere göre farkındalıklarının daha yüksek olduğu, benzer şekilde internette 8 saatten fazla zaman geçiren öğrencilerin 2-3 saat zaman geçirenlerle arasında istatistiksel olarak anlamlı bir fark olduğu ve 8 saatten fazla zaman geçirenlerin dijital veri güvenliği farkındalık puanlarının diğerlerine göre daha yüksek olduğu görülmüştür. İnternette 2-3 saat arasında zaman geçirenler ile 4-5 saat arası ve 6-7 saat arası zaman geçirenler arasında ise dijital veri güvenliği farkındalık puanları açısından anlamlı farklılık

bulunmamıştır. Üniversite öğrencilerinin dijital okuryazarlık düzeyleri ile dijital veri güvenliği farkındalık düzeylerinin arasındaki ilişkinin ele alındığı Göldağ (2021)'ın çalışması ile öğretmen adayları ile yürütülen ve katılımcıların siber bilgi güvenliği farkındalıklarının ve dijital vatandaşlık düzeylerinin değişkenler bakımından incelendiği Solmaz (2020)'ın çalışmasının bulguları, mevcut tez çalışması ile benzerdir. Aynı şekilde, ortaöğretim öğrencileri ile yürütülen dijital okuryazarlık ve bilgi güvenliği düzeylerinin ölçüldüğü Talan ve Aktürk (2021)'ün çalışması ile öğretmenlerin dijital veri güvenliği farkındalıklarının incelendiği Yılmaz ve arkadaşları (2016) tarafından yapılmış çalışmaların internette geçirilen süre değişkenine bağlı sonuçları bu tez çalışmasının bulguları ile paralellik göstermektedir. Bunun nedenleri; araştırmaların yapıldıkları dönem göz önünde alındığında mevcut tez çalışmasının pandemi döneminde yapılması olarak düşünülebilir. Pandemi döneminde uygulanan evde kal çağrısı ve dışarı çıkma kısıtlamaları nedeniyle yoğun olarak internet kullanılmıştır. Ayrıca örneklemin üniversite düzeyinde bireylerden oluşması neden olarak gösterilebilir.

Aile gelir düzeyi değişkenine göre;

Aile gelir düzeyi açısından dijital veri güvenliği farkındalık puanları incelendiğinde gelir düzeyi arttıkça farkındalık puan ortalamasının da arttığı görülmüştür. Dijital veri güvenliği farkındalık durumlarının aile gelir düzeyine göre istatistiksel olarak anlamlı farklılık gösterdiği saptanmıştır. Farklılığın, aile gelir düzeyi 5000 TL ve altında olan öğrencilerin farkındalık düzeyleri aile gelir düzeyi 7500 ve 1000 TL arasında ve 10000 TL üzerinde olanlara göre daha düşük olduğu görülmüştür. Bu bulgulara göre, aile gelir düzeyi arttıkça öğrencilerin sahip oldukları teknolojik cihaz sayısı ve türündeki artış gibi nedenlerden dolayı dijital veri güvenliği farkındalığını da arttığı düşünülebilir. Benzer araştırmalarda da aile gelir düzeyi ile dijital veri farkındalığının doğru orantılı olarak arttığı görülmektedir (Som Vural ve Kurt, 2018; Güngör ve Kurtipek, 2020; Göldağ, 2021).

"Üniversite öğrencilerinin dijital vatandaşlık düzeyleri; cinsiyet, öğrenim görmekte olduğu eğitim kademesi, sınıf, günlük ortalama internet kullanma süresi, teknolojik cihaz sahipliği, ailenin aylık ortalama gelir düzeyi değişkenlerine göre farklılık göstermekte midir?"

Cinsiyet değişkenine göre;

Üniversite öğrencilerinin dijital vatandaşlık düzeyleri cinsiyet değişkenine göre farklılaşmaktadır. Erkek öğrencilerin kadınlara göre dijital vatandaşlık puanlarının daha yüksek olduğu görülmüştür. Üniversite öğrencileri ile yürütülen ve dijital vatandaşlık göstergelerinin incelendiği Som Vural ve Kurt (2018) çalışmasında; öğretmen adaylarının katılımı ile yürütülen ve dijital vatandaşlık düzeylerinin ölçüldüğü Kocadağ (2012)'ın çalışmasının bulguları bu tez çalışması ile benzerdir. Benzer şekilde, öğrencilerin dijital vatandaşlık davranışlarını farklı değişkenlere göre inceleyen Lyons (2012)'un çalışması ile spor bilimleri fakültesi öğrencilerinin yenilikçi düzeylerinin dijital okuryazarlığa olan etkisinin incelendiği Güngör ve Kurtipek (2020) tarafından yapılan çalışmaların sonuçlarının mevcut çalışmayı desteklemektedir. Çalışmada cinsiyet değişkenine göre erkek katılımcıların lehine anlamlı farklılık olduğu saptanmıştır. Sosyal Bilgiler öğretmen adaylarının bazı değişkenlere bağlı olarak dijital vatandaşlık davranışlarının incelendiği Aslan (2016)'ın çalışması mevcut çalışmayı desteklememektedir. Öğretmen adaylarının siber bilgi güvenliği farkındalıklarının ve dijital vatandaşlık düzeylerinin değişkenlere göre incelendiği Solmaz (2020) tarafından yapılan çalışmanın da mevcut çalışmayı desteklemediği belirlenmiştir. Çalışmaların sonucuna göre cinsiyet değişkeni ile dijital vatandaşlık puanları arasında anlamlı farklılığın olmadığı bildirilmiştir. Bunun yanı sıra, dijital vatandaşlık konusunda bir ölçek geliştirmek amacıyla Jones ve Mitchell (2016)'in çalışmalarında kadınların lehine anlamlı farklılık olduğu bildirilmiştir. Ortaöğretim öğrencilerinin dijital vatandaşlık düzeyleri ile dijital okuryazarlık düzeylerinin ele alındığı Kaya (2020) tarafından yapılan çalışmada mevcut çalışmadan farklı olarak cinsiyet değişkenine göre kadın katılımcılar lehine anlamlı farklılık olduğu belirlenmiştir. Çalışmaların bazılarında dijital vatandaşlık düzeyinin erkekler lehine yüksek çıkması, bazılarında kadınlar lehine yüksek çıkması cinsiyet değişkeninin dijital vatandaşlık farkındalığı üzerinde etkili olmadığını düşündürmektedir.

Öğrenim görmekte olduğu eğitim kademesi değişkenine göre;

Eğitim kademesi değişkenine göre dijital vatandaşlık puan ortalamaları incelendiğinde, lisans öğrencilerinin ön lisans öğrencilerinden daha yüksek bir ortalamaya, yüksek lisans/doktora öğrencileriyle ise yakın bir ortalamaya sahip olduğu görülmektedir. Eğitim kademesi değişkenine göre öğrencilerin dijital vatandaşlık puan ortalamaları arasındaki farkın istatistiksel olarak anlamlı olduğu sonucuna ulaşılmıştır. Lisans ve yüksek lisans/doktora öğrencilerinin vatandaşlık puanlarının ön lisans

öğrencilerinden daha yüksek olduğu görülmüştür, lisans ve yüksek lisans/doktora öğrencileri arasında ise fark bulunmamıştır. Elde edilen bu bulguya göre, eğitim kademesinin bireylerin dijital vatandaşlık düzeyine etki edebileceği söylenebilir. Bireylerin eğitim kademesi arttıkça dijital vatandaşlık alanında daha fazla bilgi sahibi oldukları, bunu daha fazla önemsedikleri düşünülebilir.

Sınıf düzeyi değişkenine göre;

Sınıf düzeylerine göre dijital vatandaşlık ortalamaları incelendiğinde, sınıf düzeyi arttıkça ortalamanın da arttığı görülmüştür. Katılımcıların sınıf düzeyine göre dijital vatandaşlık puan ortalamaları arasında fark olup olmadığı incelendiğinde, bir fark olduğu ve bu farkın istatistiksel olarak anlamlı olduğu sonucuna ulaşılmıştır. Dördüncü sınıflarda, birinci ve ikinci sınıflara göre dijital vatandaşlık puanlarının daha yüksek olduğu, sınıf düzeyi arttıkça dijital vatandaşlık düzeyinin de arttığı görülmüştür. Üniversite öğrencileri ile yürütülen ve dijital vatandaşlık göstergelerinin değerlendirildiği Som Vural ve Kurt (2018)'ın çalışması mevcut çalışmayı desteklemektedir. Farklı değişkenlere göre öğrencilerin dijital vatandaşlık davranışlarını inceleyen Lyons (2012) tarafından yürütülen çalışmanın bulguları da mevcut çalışmayı destekler niteliktedir. Lisans düzeyinde sınıf düzeyi arttıkça dijital vatandaşlık davranışlarının da artış göstermesi, 1.sınıfta okutulan Bilişim Teknolojileri, 2.sınıfta okutulan İnsan ve Bilgisayar Etkileşimi, Bilgisayar Destekli Eğitim, 3.sınıf Bilgisayar, Bilgisayar İşletim Sistemleri, Bilgisayar Destekli Eğitim, Bilgisayar Ağları ve Güvenliği, Bilgisayar Kullanımı, Bilgisayar Etkileşimi ve Kullanılabilirlik Analizi gibi derslerden kaynaklı olduğu düşünülmektedir.

İnternette geçirilen süre değişkenine göre;

Araştırmanın bulgularına göre; internette geçirilen süre bakımından 118 kişi 1 saatten az, 446 kişi en az 2 en fazla 3 saat, 838 kişi en az 4 en fazla 5 saat, 632 kişi 6-7 saat arası ve 460 kişi 8 saatten fazla zaman geçirdiğini bildirmişlerdir. internette 1 saatten az ve 8 saatten fazla zaman geçirenlerin diğer kişilere göre farkındalık puan ortalamalarının daha yüksek olduğu gözlenmiştir. Katılımcıların dijital vatandaşlık puan ortalamaları arasında internette geçirilen süreye göre istatistiksel olarak anlamlı bir farklılık olduğu görülmüştür. İnternette 0-1 saat arası zaman geçiren kişilerin 2-3 saat zaman geçirenlere göre dijital vatandaşlık eğilimlerinin daha yüksek olduğunu

göstermektedir. Benzer şekilde internette 8 saatten fazla zaman geçiren öğrencilerin 2-3 saat zaman geçirenlerle arasında istatistiksel olarak anlamlı bir fark olduğu görülmüştür. Ayrıca 8 saatten fazla zaman geçirenlerin dijital vatandaşlık puanlarının diğerlerine göre daha yüksek olduğu görülmüştür. İnternette 2-3 saat arasında zaman geçirenler ile 4-5 saat arası ve 6-7 saat arası zaman geçirenler arasında ise dijital vatandaşlık puanları açısından anlamlı farklılık bulunmamıştır. Çakmak ve Aslan (2018)'ın, Sakallı ve Çiftçi (2016)'nin, Kocadağ (2012)'ın, Onursoy (2018)'un çalışmalarının mevcut çalışmanın bulguları ile paralellik gösterdiği görülmektedir. Öğretmen adaylarının katılımı ile yapılan, katılımcıların siber bilgi güvenliği farkındalıklarının ve dijital vatandaşlık düzeylerinin değişkenlere göre incelendiği Solmaz (2020)'ın çalışması da mevcut çalışma ile çelişmektedir. Sosyal Bilgiler öğretmen adaylarının dijital vatandaşlık göstergelerinin incelendiği Dere ve Yavuzay (2019)'ın çalışmasının da mevcut tez çalışması ile çeliştiği görülmektedir. Mevcut çalışmanın bulguları ile bu çalışmalar arasındaki farklılığın, katılımcıların üniversitelerin farklı öğretim kademelerinde bulunmalarından, kullanılan veri toplama araçlarından kaynaklanabileceği düşünülebilir. Çalışmalar ağırlıklı olarak üniversite öğrencileri ile yapılmış olsa da genelde farklı bölümlerden öğretmen adaylarından oluşmaktadır. Mevcut tez çalışmasında ise örneklemi üniversitede farklı bölümlerde öğrenim gören öğrenciler oluşturmaktadır. Bu durumun katılımcıların internette geçirdikleri süreyi etkileyebileceği düşünülmektedir.

Aile gelir düzeyi değişkenine göre;

Aile gelir düzeyi açısından dijital vatandaşlık puanları incelendiğinde gelir düzeyi arttıkça vatandaşlık puan ortalamasının da arttığı görülmüştür Dijital vatandaşlık durumlarının aile gelir düzeyine göre istatistiksel olarak anlamlı farklılık gösterdiği saptanmıştır. Aile gelir düzeyi 5000 TL ve altında olan öğrencilerin dijital vatandaşlık eğilimleri aile gelir düzeyi 7500 ve 1000 TL arasında ve 10000 TL üzerinde olanlara göre daha düşük olduğu görülmüştür. Buna göre aile gelir düzeyi arttıkça dijital vatandaşlık eğiliminin de arttığı söylenebilir. Kocadağ (2012) tarafından yapılan çalışmada mevcut çalışmayı destekler niteliktedir. Çalışmada, aile ortalama gelir düzeyi ile dijital vatandaşlık puanları arasında anlamlı farklılık olduğu belirlenmiştir. Bu farklılığın aile gelir düzeyi arttıkça katılımcıların daha kolay teknolojik cihaz sahibi olabilmelerine ve sahip oldukları teknolojik cihazların türüne dayandırılması mümkündür.

"Dijital vatandaşlık farkındalığının ve bilgi düzeyinin artırılmasıyla ilgili olarak, öğrencilerin üniversite yönetiminden beklentileri nelerdir?"

Çalışma kapsamında üniversite öğrencilerine dijital vatandaşlık konusunda farkındalığın ve bilgi düzeyinin artırılmasıyla ilgili olarak üniversite yönetiminden beklentilerinin neler olduğu sorulmuştur 2500 katılımcıdan 1265 öğrenci soruya yanıt vermiştir. Verilen yanıtlar incelendiğinde; öğrenciler dijital vatandaşlık konusunda bilgilerinin kısıtlı olduğunu ve beklentilerinin ders, seminer ya da konferans ile bilgilendirme yapılması yönünde belirtmişlerdir. Bu tez çalışmasının yürütüldüğü üniversitede dijital vatandaşlık ile ilişkili ders olmamasına karşılık, öğrencilerin dijital vatandaşlık farkındalık düzeylerinin yüksek çıkması dikkat çekicidir. Daha da dikkat çekici ve sevindirici olan husus, öğrencilerin bu konuda bilgilendirilmeyi istediğini ifade etmeleridir.

"Dijital veri güvenliği konusunda farkındalığın ve bilgi düzeyinin artırılmasıyla ilgili olarak, öğrencilerin üniversite yönetiminden beklentileri nelerdir?"

Çalışma kapsamında üniversite öğrencilerine dijital veri güvenliği konusunda farkındalığın ve bilgi düzeyinin artırılmasıyla ilgili olarak üniversite yönetiminden beklentilerinin neler olduğu sorulmuştur. 2500 katılımcıdan 1395 öğrenci soruya yanıt vermiştir. Verilen yanıtlar incelendiğinde; öğrenciler üniversite yönetiminden de bu konularda ders açılması, seminer ya da konferans ile bilgilendirme yapılmasını istediklerini ifade etmişlerdir. Mevcut tez çalışmasının yürütüldüğü üniversitede dijital veri güvenliği farkındalığı ile ilişkili derslerin sadece Yönetim Bilişim Sistemleri ve Bilgisayar Mühendisliği yüksek lisans bölümünde olduğu görülmüştür. Bu bölümlerde öğrenim gören öğrencilere Bilgisayar Ağları ve Güvenliği, Bilgi Gizleme Teknikleri ve Ağ Güvenliği dersleri okutulmaktadır. Ancak üniversite genelinde öğrencilerin tamamı düşünülerek dijital veri güvenliğine ilişki bir ders bulunmamaktadır. Buna karşılık, öğrencilerin dijital veri güvenliği farkındalık düzeylerinin yüksek çıktığı görülmektedir. Öğrencilerin dijital veri güvenliğine verdikleri önemden dolayı bilgilendirilmeyi istedikleri, beklentilerinin bu yönde olduğu önemli bir bulgudur.

BÖLÜM 6

SONUÇ VE ÖNERİLER

Tez çalışmasında sonuç olarak; üniversite öğrencilerinin dijital vatandaşlık ve dijital veri güvenliği farkındalık düzeyleri arasında istatistiksel olarak anlamlı bir ilişki olduğu belirlenmiştir. Ayrıca, üniversite öğrencilerinin dijital vatandaşlık ve dijital veri güvenliği farkındalık düzeylerinin yüksek düzeyde olduğu görülmüştür. Dijital vatandaşlık ve dijital veri güvenliği farkındalığı düzeylerinin demografik değişkenlere göre değişimini incelemek üzere gerçekleştirilen istatistiksel analizlerde cinsiyet, sınıf düzeyi, öğrenim görmekte olduğu eğitim kademesi, günlük ortalama internet kullanma süresi ve ailenin aylık ortalama gelir düzeyi değişkenleri ele alınmıştır. İstatistiksel analizler sonucunda; dijital veri güvenliği farkındalığı düzeyleri bakımından cinsiyet, aile gelir düzeyi, eğitim kademesi, internette geçirilen süre değişkenleri arasında anlamlı farklılık olduğu belirlenmiştir. Dijital vatandaşlık düzeyleri bakımından cinsiyet, aile gelir düzeyi, eğitim kademesi, sınıf düzeyi ve internette geçirilen süre değişkenleri arasında anlamlı farklılık olduğu görülmüştür.

Toplumların dijital vatandaşlık ve dijital veri güvenliği farkındalık düzeylerinin yüksekliğinde başta hükümet politikaları olmak üzere öğretmenler, eğitim öğretim kurumu yöneticileri gibi bireyleri hayata hazırlayan, bu alanda bilinçlendiren unsurlar önem arz etmektedir. Günümüzde internet, bilgisayar, iletişim ağlarının kullanımının her geçen gün artması beraberinde teknolojik güvenlik ve dijital veri güvenliğini daha önemli konuma getirmiştir. Bilginin elektronik ortamda üretimi ve sunumu sağladığı avantajlar yanında çeşitli güvenlik sorunlarının yaşanmasında rol oynamaktadır. Bireylerin bu tür sorunlardan ve zararlarından korunmaları için tehlikelerin bilincinde olmaları önemli bir husus olmaktadır. Bunun sağlanması ise eğitim ve bilinçlendirme aracılığıyla

gerçekleşebilmektedir. Bu kapsamda araştırmada ulaşılan bulgular doğrultusunda yazar tarafından uygulayıcılara ve araştırmacılara yönelik aşağıdaki önerilerde bulunulmuştur:

Uygulayıcılara Yönelik Öneriler

Öğrencilerin teknolojinin hatalı kullanımından, bilgi eksikliklerinden kaynaklanabilecek zararların azaltılması amaçlanmalıdır. Bu kapsamda öğrencilerin dijital vatandaşlık ve dijital veri güvenliği farkındalıklarının oluşturulması, veri güvenliği faaliyetlerine ilişkin bilinçlendirme, faaliyetlerin benimsetilmesi ve uygulatılmasına önem verilmelidir. Öğrenciler interneti temel bilgi kaynağı olarak görmektedirler. Bundan dolayı, güvenli bir şekilde dijital içerikleri nasıl bulabilecekleri, oluşturacakları, tüketecekleri, iletecekleri ve paylaşım yapabilecekleri öğretilmelidir.

Öğrencilerin dijital vatandaşlık ve dijital veri güvenliği farkındalıklarının oluşturulması amacıyla, müfredata derslerin eklenmesi gündeme gelmelidir.

Öğrencilere yönelik dijital vatandaşlık ve dijital veri güvenliği farkındalığı hususunda el kitapçıkları, posterler, broşürler hazırlanması faydalı olabilir. Ayrıca üniversiteler bu konuda sunumlar, seminerler, videolar hazırlayabilir ve öğrencilere ulaştırabilir.

Eğitim öğretim kurumlarında görev yapan akademisyenlere ve yöneticilere de dijital vatandaşlık ve dijital veri güvenliği farkındalık düzeyini arttırmaya yönelik hizmet içi eğitimler verilebilir.

Araştırmacılara Yönelik Öneriler

Bu araştırma Trakya Üniversitesi'nde öğrenim gören öğrencilerle yürütülmüştür. Geniş çaplı katılımların olacağı bölgesel ve ulusal araştırmalar yapılabilir. Farklı demografik özelliklere sahip örneklem grupları ile yapılacak çalışmaların sonucunda daha kapsamlı bilgilere ulaşılabilir.

Özel üniversite ve devlet üniversitelerinde öğrenim gören öğrencilerle çalışılarak arada fark olup olmadığına bakılabilir.

Bölüm bazında farklılık olup olmadığı ve nedenlerin belirlenmesine yönelik çalışmalar yapılabilir.

Üniversite öğrencilerinin dijital vatandaşlık ve dijital veri güvenliği farkındalık düzeylerini etkileyen başka değişkenlerin olup olmadığı araştırılabilir.

Bu araştırmalardan elde edilen bulgular ışığında; ilgili düzeyleri artıran değişkenlerin iyileştirilmesi, azaltan değişkenlerin ise ortadan kaldırılmasına yönelik adımlar atılabilir.

Üniversite öğrencileri ile yürütülen bu çalışmanın diğer eğitim kademelerindeki öğrencilerle, yeni mezun öğrencilerle ve farklı yaş grupları ile yapılması, diğer bir ifade ile toplumdaki her kesimi kapsayacak şekilde çalışmaların yapılması önerilebilir. Bu sayede toplumdaki bireylerin dijital veri güvenliği farkındalıkları daha net olarak ortaya konabilir.

Bu alanda nitel çalışmaların yürütülmesi daha derinlemesine verilere ulaşılmasını sağlayabilir. Üniversite öğrencileri ile yapılacak mülakatlar sonucunda veri güvenliği farkındalıklarına ilişkin önemli bulgular sunabilir.

KAYNAKLAR

Akça, E.B., ve Kaya, B. (2016). Toplumsal cinsiyet eşitliği perspektifinden dijital bölünme ve farklı yaklaşımlar, *Intermedia International e-Journal*, Fall, /3(5).

Akıncı, A.N. (2019). Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti, Uzmanlık Tezi, T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Yayın No: 0001, Ankara.

Aldemir, C., ve Avşar, M., (2020). Pandemi döneminde dijital vatandaşlık uygulamaları. *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi*, COVID-19 ÖZEL SAYISI 2, 148-169.

Alıcı, Y. (2017). *Bankacılık Kanunu Şerhi*, İstanbul, On İki Levha.

Altın, H.M., ve Kalelioğlu, F. (2015). Fatih projesi ile ilgili öğrenci ve öğretmen görüşleri. *Baskent University Journal of Education*. 2(1), 89-105.

Arcagök, S. (2020). Öğretmenlerin dijital vatandaşlığa yönelik algılarının incelenmesi. *Yüzüncü Yıl Üniversitesi Eğitim Fakültesi Dergisi*, 17 (1), 534-556. DOI: 10.33711/yyuefd.693832.

Arıtürk, M. (2015). Bilgi farkındalığı ve bilgi güvenliğinin karşılaştırılması. *XVII. Akademik Bilişim Konferansı*, 4-6 Şubat 2015, Anadolu Üniversitesi, Eskişehir.

Aslan, A. (2016). *The Changes in Safer Internet Use of Children in Turkey between the years of 2010-2015 and Impacts of Related Implementations*. Doctoral Dissertation. Atatürk University Institute of Educational Sciences. http://eukidsonline.metu.edu.tr/file/EUKO_Turkey2015_SummaryReport.pdf, Erişim Tarihi: 22.02.2022.

Aslan, S. (2016). *İlköğretim Sosyal Bilgiler Öğretmen Adaylarının Dijital Vatandaşlık Davranışlarının Bazı Değişkenler Açısından İncelenmesi (Fırat, Dicle, Siirt, Adıyaman Üniversiteleri Örneği)*. (Yayımlanmamış Yüksek Lisans Tezi), Fırat Üniversitesi, Elâzığ.

Aslay, F., Çam, H., ve Özen, Ü. (2019). Yükseköğretim kurumlarında bilgi güvenliği farkındalık düzeylerinin ölçümlenmesi. *Yönetim Bilişim Sistemleri Dergisi*, 5 (2), 1-11.

Avcı, Ü. ve Oruç, O. (2020). Üniversite öğrencilerinin kişisel siber güvenlik davranışları ve bilgi güvenliği farkındalıklarının incelenmesi. *İnönü Üniversitesi Eğitim Fakültesi Dergisi*, 21(1), 284-303. doi: 10.17679/inuefd.526390.

Aydemir, M. (2019). Yenilenen sosyal bilgiler dersi öğretim programının dijital vatandaşlık ve alt boyutları açısından incelenmesi. *Uluslararası Güncel Eğitim Araştırmaları Dergisi,* 4 (2), 15-38.

Aydın, A. (2015). Dijital Vatandaşlık. *Türk Kütüphaneciliği*, 29(1), 142-146.

Aygün, M. (2019). *Sosyal Bilgiler Öğretmenlerinin Sosyal Bilgiler Öğretmen Adaylarının Dijital Vatandaşlık Durumlarının İncelenmesi*. Yayımlanmamış Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, İstanbul.

Bakır, E. (2016). *Sınıf Öğretmeni Adaylarının Dijital Vatandaşlık Seviyelerinin Dijital Vatandaşlık Alt Boyutlarına Göre İncelenmesi*. (Yayımlanmamış Yüksek Lisans Tezi), Karadeniz Teknik Üniversitesi, Trabzon.

Başalp, N. (2015). Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri, *MÜHF-HAD*, 21(1), 77-105.

Bayer, İ. (2018). Çocuklar İçin Dijital Gelecek: DQ World Türkçeleşiyor. https://dijitalmedyavecocuk.bilgi.edu.tr/2018/04/09/cocuklar-icin-dijital-gelecek-dqworld/, Erişim Tarihi: 22.02.2022.

Baykara, M., Daş, R. ve Karadoğan, İ. (2013). Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi. 1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu, (ISDFS'13), 231-239. Elâzığ, Türkiye. http://web.firat.edu.tr/mbaykara/bg.pdfr.e, Erişim Tarihi: 22.02.2022.

Berardi, R. P. (2015). *Digital citizenship: elementary educator perceptions and formation of instructional value and efficacy*, (Yayımlanmamış doktora tezi). Immaculata University, Philadelphia, https://www.researchgate.net/publication/305048751_DIGITAL_CITIZENSHIP_ELEMENTARY_EDUCATOR_PERCEPTIONS_AND_FORMATION_OF_INSTRUCTIONAL_VALUE_AND_EFFICACY, Erişim Tarihi: 12.02.2022.

Bıkmaz, Z (2017). Sağlık yönetimi bölümü öğrencilerinin mobil güvenlik farkındalığı ve dijital veri güvenliği farkındalıklarının belirlenmesi. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi,* 1(1), 22-30.

Bilinçli İnternet Hareketi Projesi, (2022). http://www.eba.gov.tr/video/izle/3520699587a67ccde43feb5b1ed742b021b79f2b04004, Erişim Tarihi: 22.02.2022.

Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö., Karadeniz, Ş., Demirel, F. (2015). *Bilimsel Araştırma Yöntemleri.* (19.Baskı). Ankara: PegemA Yayıncılık.

Candemir, A. (2020). Bankacılık Sektöründe Kişisel Verilerin Korunması Alanında Yaşanan Gelişmeler, https://blog.lexpera.com.tr/bankacilik-sektorunde-kisisel-verilerin-korunmasi-alaninda-yasanan-gelismeler/, Erişim Tarihi: 27.02.2022.

Choi, M. (2016). A Concept analysis of digital citizenship for democratic citizenship education in the internet age, *Theory & Research in Social Education*, 44:4, 565-607, DOI: 10.1080/00933104.2016.1210549.

Choi, M., Cristol, D. ve Gimbert, B. (2018). Teachers as digital citizens: The influence of individualbackgrounds, İnternet use and psychological characteristics onteachers'levels of digital citizenship. *Computers & Education,* 121, 143-161.

Choi, M., Glassman, M. ve Cristol, D. (2017). What it means to be a citizen in the İnternet age: Development of a reliable and valid digital citizenship scale. *Computers & education*, 107, 100-112.

Civelek, Y.D. (2011). *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi*. Planlama Uzmanlığı Tezi. Ankara, Yayın No: 2821, DPT.

Coşkun, B.; ve Yıldırım, Ç. P. (2019). "Kolluk Hizmetinden Siber Güvenliğe: Güvenlik Yönetiminde Değişim", *13.Uluslararası Kamu Yönetimi Sempozyumu* (KAYSEM13), (Nisan 18-20, Gaziantep), 1555-1566.

Çakır, S. ve Kesler, M. (2012). Bilgisayar güvenliğini tehdit eden virüsler ve antivirüs yazılımları. XIV. Akademik Bilişim Konferansı Bildirileri, 551-558. https://ab.org.tr/ab12/bildiri/82.pdf., Erişim Tarihi: 22.02.2022.

Çakmak, V. (2016). Çocuk ve dijital oyun etkileşimine etiksel bir bakış. *ICHACS*, 1(1), 430.

Çakmak, Z. ve Aslan, S. (2018). Sosyal bilgiler öğretmen adaylarının dijital vatandaşlık davranışlarının bazı değişkenler açısından incelenmesi. *Adıyaman Üniversitesi Eğitim Bilimleri Dergisi*, 8(1), 72-99.

Çebi, A. (2020). *Dijital Yeterlik: Dijital Çağda Dönüşüm Yolculuğu* (2. Baskı). Ankara: Pegem Akademi.

Çetin, H. (2014). Kişisel veri güvenliği ve kullanıcıların farkındalık düzeylerinin incelenmesi. *Akdeniz İİBF Dergisi*, 14 (29), 86-105

Çubukçu, A. ve Bayzan, Ş. (2013). Türkiye'de dijital vatandaşlık algısı ve bu algıyı internetin bilinçli, güvenli ve etkin kullanımı ile artırma yöntemleri. *Middle Eastern & African Journal Of Educational Research*, 5, 148-174.

Dağsalı, A. (2019). Kişisel Verilerin Korunması Kanununun Uygulanma Süreci, http://yasaizleme.org.tr/kisisel-verilerin-korunmasi-kanununun-uygulanma-sureci/, Erişim Tarihi: 26.02.2022.

Demirer, V., ve Dikmen, C.H. (2018). Öğretmenlerin FATİH projesine yönelik görüşlerinin teknolojik pedagojik alan bilgisi bağlamında incelenmesi. *İlköğretim Online*. 17(1), 26-46.

Dere, İ., ve Yavuzay, M. (2019). Sosyal bilgiler öğretmen adaylarının dijital vatandaşlık göstergelerinin incelenmesi. *MANAS Sosyal Araştırmalar Dergisi*, 8 (3), 2400-2414.

Dixon, Laura; Correa, Teresa vd. (2014). Gendered space: the digital divide between male and female users in internet public access Sites. Journal of Computer-Mediated Communication, 19, 991– 1009.

Dönmez, O., Odabaşı, H. F., Kabakçı Yurdakul, I., Kuzu, A. ve Girgin, Ü. (2014). Öğretmen adayları için hazırlanan algılanan internet riskleri ölçeğinin güvenirlik ve geçerlik çalışmaları. *8. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu*, 18-20 Eylül 2014, Trakya Üniversitesi, Edirne.

DQ World, (2022). DQ World Nedir, https://www.dqworld.net/lang:tr/#!/landing/whatisdqworld, Erişim Tarihi: 19.02.2022.

DQI, (2022). Who's advancing Digital Intelligence, https://www.dqinstitute.org/aboutus/#who_we_are, Erişim Tarihi: 22.02.2022.

Dülger, M.V., ve Özkan, O. (2021). Sosyal medya yasası Meclis'ten geçti: Peki, ya şimdi?, https://www.researchgate.net/publication/349552885, Erişim Tarihi: 27.02.2022.

Education, Alberta. (2012). *Digital Citizenship Policy Development Guide*. Edmonton, Canada: Alberta Education School Technology Branch. https://education.alberta.ca/media/3227621/digital-citizenship-policy-development-guide.pdf, Erişim Tarihi: 25.02.2022.

Elçi, A. C. ve Sarı, M. (2016). Bilişim teknolojileri ve yazılım dersinde dijital vatandaşlık: bir ölçek geliştirme çalışması. *Journal of Human Sciences,* 13(2), 3602-3613.

Elektronik Haberleşme Kanunu, (2008). 5809 Sayılı Elektronik Haberleşme Kanunu, https://www.resmigazete.gov.tr/eskiler/2008/11/20081110M1-3.htm, Erişim Tarihi: 27.02.2022.

E-Nabız, (2022). https://enabiz.gov.tr/Yardim/Index, Erişim Tarihi: 20.02.2022.

Ereş, F. (2015). Vatandaşlık eğitimi ve karakter eğitimi politikalarının değerlendirilmesine yönelik nitel bir çalışma. *Mehmet Akif Ersoy Üniversitesi Eğitim Fakültesi Dergisi,* 36, 120-136.

Esenyel Hanaz, F. (2021). Çevrimiçi eğitimde üniversite öğrencilerinin kişisel verilerinin işlenmesinin hukuki sebepleri, *TBB Dergisi,* http://tbbdergisi.barobirlik.org.tr/m2021-155-1992, Erişim Tarihi: 28.02.2022.

EuKids Online, (2020). Avrupa Çevrimiçi Çocuklar Projesi. https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/participant-countries/turkey/TurkeyExecSum.pdf, Erişim Tarihi: 23.02.2022.

Farooq, A., Isoaho, J., Virtanen, S., ve Isoaho, J. (2015). Information security awareness in educational institution: An analysis of students' individual factors. *In 2015 IEEE Trustcom/BigDataSE/ISPA* (Vol. 1, 352-359). IEEE.

Fatih Projesi, (2019). Fırsatları Artırma ve Teknolojiyi İyileştirme Hareketi. http://fatihprojesi.meb.gov.tr/, Erişim Tarihi: 23.02.2022.

Filiz, O. (2020). Dijital Güvenlik, A. A. Kurt ve F. Odabaşı (Ed.) *Pandemi Döneminde Sınanan Dijital Vatandaşlık* içinde (135-172). Ankara: Anı.

Fingal, D. (2017). Infographic: Citizenship in the digital age. https://www.iste.org/explore/digital-citizenship/infographic-im-digital-citizen. Erişim tarihi: 15.02.2022.

Fuster, G. G, (2014). The emergence of personal data protection as a fundamental right of the EU, Springer, *The Cambridge Law Journal*, 74(02), 374-375.

Girardin, L. (2020). The 7 Barrıers To Dıgıtal Communıcatıon, https://www.govloop.com/community/blog/7-barriers-digital-communication/, Erişim Tarihi: 20.02.2022.

Gökçearslan, Ş., Günbatar, M. S., ve Sarıtepeci, M. (2021). Ortaöğretim öğrencilerinin bilgi güvenliği farkındalıklarının incelenmesi. *Yüzüncü Yıl Üniversitesi Eğitim Fakültesi Dergisi,* 18(1), 354-373.

Göldağ, B. (2021). Üniversite öğrencilerinin dijital okuryazarlık düzeyleri ile dijital veri güvenliği farkındalık düzeyleri arasındaki ilişkinin incelenmesi. *e-Uluslararası Eğitim Araştırmaları Dergisi,* 12 (3), 82-100. DOI: 10.19160/e-ijer.950635.

Görmez, E. (2016). Öğretmen adaylarının" dijital vatandaşlık ve alt boyutları" hakkındaki görüşleri (bir durum çalışması). *Electronic Turkish Studies*, 11(21).

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. ve Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73, 345-358.

Gündüzalp, C. (2021). Üniversite çalışanlarının dijital veri ve kişisel siber güvenlik farkındalıkları (Bilgi İşlem Daire Başkanlıkları Örneği). *Journal of Computer and Education Research*, 9 (18), 598-625. DOI: 10.18009/jcer.907022.

Güngör, N. B., ve Kurtipek, S. (2020). Spor bilimleri fakültesi öğrencilerinin bireysel yenilikçilik düzeyinin dijital okuryazarlığa etkisinin yapısal eşitlik modeli ile incelenmesi. *Journal of Human Sciences,* 17(2), 756-767. https://doi.org/10.14687/jhs.v17i2.6021., Erişim Tarihi: 25.02.2022.

Haeussinger, F., ve Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior. Thirty Fourth International Conference on Information Systems, Milan 2013.

Hanaylı, M. C., Sebetci, Ö., Topal, A. ve Gürel Dönük, G. (2018). Dijital ortamda kişisel veri güvenliği ve sosyal medya reklamcılığı üzerine bir değerlendirme, *Kesit Akademi Dergisi*, (16), 389-409.

Henkoğlu, T. (2017). Veri Koruma Kanununun Getirdikleri, What Data Protection Law Brings in, *Journal of Current Researches on Social Sciences*, 7 (2), 241-250.

Henkoğlu, T., ve Yılmaz, B., 2013. Avrupa Birliği AB bilgi güvenliği politikaları. *Türk Kütüphaneciliği,* 27 (3), 451-471.

HES Uygulaması, (2019). https://hayatevesigar.saglik.gov.tr/HES.pdf, Erişim Tarihi: 20.02.2022.

Hollandsworth, R., Dowdy, L., ve Donovan, J. (2011). Digital Citizenship in K-12: It Takes a Village. *TechTrends*, 55, 37-47. https://doi.org/10.1007/s11528-011-0510-z., Erişim Tarihi: 27.02.2022.

https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler, Erişim Tarihi: 28.02.2022.

https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=13078&MevzuatTur=7&MevzuatTertip=5, Erişim Tarihi: 27.02.2022.

https://www.resmigazete.gov.tr/eskiler/2010/07/20100728-9.htm, Erişim Tarihi: 27.02.2022.

https://www.resmigazete.gov.tr/eskiler/2016/05/20160505.pdf, Erişim Tarihi: 28.02.2022.

https://www.resmigazete.gov.tr/eskiler/2020/02/20200225-12.htm, Erişim Tarihi: 27.02.2022.

https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm, Erişim Tarihi: 27.02.2022.

https://www.resmigazete.gov.tr/eskiler/2020/12/20201204-13.htm, Erişim Tarihi: 27.02.2022.

International Society for Technology, (2020). https://www.iste.org/ Erişim tarihi: 20.02.2022.

İzmir Üniversiteleri Platformu, (2019). https://www.izmiruniversiteleri.com/2019-sosyal-sorumluluk-projeleri/, Erişim Tarihi: 22.02.2022.

Jeske, D. and Van Schaik, P. (2017). Familiarity with ınternet threats: Beyond awareness. *Computers & Security*, 66, 129-141.

Jones, L., ve K. Mitchell, (2015). "Defining and measuring youth digital citizenship". *New Media&Society* 9 (18), 2063-2079.

Kara, M., 2018. *Kurumsal Bilgi Güvenliği Teknik ve Yönetimsel Yöntemleriyle*. İstanbul: Papatya Yayıncılık.

Karaduman, H. (2011). 6*. sınıf sosyal bilgiler dersinde dijital vatandaşlığa dayalı etkinliklerin öğrencilerin dijital ortamdaki tutumlarına etkisi ve öğrenme öğretme sürecine yansımaları.* Yayınlanmamış doktora tezi. Eskişehir Anadolu Üniversitesi.

Karaduman, H. Öncül, B. (2019). Kuramsal temeller ve güncel tartışmalar ışığında 21.yüzyıl vatandaşlık ve vatandaşlık eğitimi. Öztürk, C., İbrahimoğlu, Z., Yıldırım, G. (Ed.). *Dijital vatandaşlık ve dijital vatandaşlık eğitimi*. Ankara: Pegem Akademi.

Karaduman, H. ve Öztürk, C. (2014). Sosyal bilgiler dersinde dijital vatandaşlığa dayalı etkinliklerin öğrencilerin dijital vatandaşlık tutumlarına etkisi ve dijital vatandaşlık anlayışlarına yansımaları. *Journal of Social Studies Education Resarch*, 5(1), 38-78.

Karasar, N. (2020). *Bilimsel Araştırma Yöntemi: Kavramlar İlkeler Teknikler*. (35. Baskı). Ankara: Nobel Akademik.

Kaya, A. ve Kaya, B. (2014). Öğretmen adaylarının dijital vatandaşlık algısı. *International Journal of Human Sciences,* 11(2), 346-361.

Kaya, M. (2020). *Ortaöğretim Öğrencilerinin Dijital Vatandaşlık ve Dijital Okuryazarlık Düzeyleri Arasındaki İlişkinin İncelenmesi*. (Yayımlanmamış Yüksek Lisans Tezi). Mersin Üniversitesi, Mersin.

Kaya, Ö.F., ve Öztürk, E. (2017). Veri ve ağ güvenliği için uygulama ve analiz çalışmaları. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, 16(31), 85-102.

Keleş, M. K. ve Güneş, A. (2013). 24 bit renkli dokümanların farklı biyometri teknoloji kullanılarak güvenliğinin sağlanması. *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı,* 20-21 Eylül 2013, Ankara.

Kılınç, D. (2012). Anayasal Bir Hak Olarak Kişisel Verilerin Korunması, *AÜHFD*, 61(3), 1089-1170.

Kılınç, D. (2016) "5651 sayılı internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında Kanun'un 9/A maddesi çerçevesinde özel hayatın korunması", *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi,* 20(2), 577-624.

Kınay, H., Sözcü, Ö. F., Taşkın, E. ve İpek, Ġ. (2014). Bilgi güvenliği farkındalığı ölçeğinin ilk bulguları. *8. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu*, 18-20 Eylül 2014, Trakya Üniversitesi, Edirne.

Kilci, Z. (2019). *Sosyal bilgiler öğretmenlerinin dijital vatandaşlığa yönelik görüşleri ve uygulamaları,* Yayımlanmamış yüksek lisans tezi, Sosyal Bilgiler Eğitimi Programı Türkçe ve Sosyal Bilimler Eğitimi Anabilim Dalı, Eskişehir.

Kocadağ T. (2012). *Öğretmen adaylarının dijital vatandaşlık düzeylerinin belirlenmesi.* (Yüksek Lisans Tezi) Karadeniz Teknik Üniversitesi Eğitim Bilimleri Enstitüsü, Trabzon.

Korkmaz, E.V. (2018). Üniversite öğrencilerinin internet ve veri güvenliği farkındalıkları. *Journal of Social And Humanities Sciences Research (JSHSR)*, 5(25), 2222-2229.

Korucu, O. (2021). *Veri Güvenliğinin İyileştirilmesi Sürecinde Risk Tabanlı Küresel Standart, Çerçeve ve En İyi Uygulama Yaklaşımları*, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, İstanbul.

Kritof, T., Zlatan, M., ve Luka M. (2018). Human digital index. *International Journal of Digital Technology & Economy*, 3, 2, 95-122.

Kruger, H., Drevin, L. ve Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*,18(5), 316- 327.

Kurt, A., Günüç, S., Ersoy, M. (2013). The current state of digitalization: Digital Native, Digital Immigrant and Digital Settler. *Ankara University Journal of Faculty of Educational Sciences (JFES),* 46 (1), 1-22.

Küzeci, E. (2019). *Kişisel Verilerin Korunması,* Yenilenmiş ve Gözden Geçirilmiş 3. Baskı, Ankara: Turhan.

KVKK. (2016). https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf, Erişim Tarihi: 25.02.2022.

Lindsey, L. (2015). *Preparing Teacher Candidates for 21. Century Classrooms: A Study of Digital Citizenship*. Yayımlanmamış Doktora Tezi, Arizona State University, Arizona.

Lyons, B. (2012). Solidarity children and research, *Special Issue: The role of solidarity in bioethics*, 26(7), 369-375, https://doi.org/10.1111/j.1467-8519.2012.01988.x

Mart, İ. (2012). *Bilişim kültüründe bilgi güvenliği farkındalığı*. Yayımlanmamış yüksek lisans tezi. Kahramanmaraş Sütçü İmam Üniversitesi, Kahramanmaraş.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., ve Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior,* 69, 151-156.

Mediapharm (2019). The data security awareness programme. Retrieved from https://www.mediapharm.co.uk/blog/data-security-awareness, Erişim Tarihi: 23.02.2022

Mercimek, B., Yaman, N., Kelek, A., ve Odabaşı, H. (2016). Dijital dünyanın yeni gerçeği: troller, *Trakya Üniversitesi Eğitim Fakültesi Dergisi*, 6(1), 67-77.

MHRS, (2022). Hakkımızda, https://www.mhrs.gov.tr/hakkimizda.html, Erişim Tarihi: 22.02.2022.

Mısırlı, Ö. (2020). *Dijital İletişim*, A. A. Kurt, F. Odabaşı (Ed.) Pandemi Döneminde Sınanan Dijital Vatandaşlık içinde (87-106). Ankara: Anı Yayıncılık.

Moeller, S., Joseph, A., Lau, J. ve Carbo, T. (2011). *Towards Media and Information Literacy Indicators.* UNESCO: Paris.

Mossberger, K., Tolbert, C. J., and Hamilton, A. (2012). Measuring digital citizenship: Mobile access and broadband. *International Journal of Communication*, 6, 2492-2528.

Netwong, T. (2016). The using of the moodle e-learning management system at suan dusit university to develop digital citizenship and learning achievement in information technology. *Asean Journal of Education*, 2(2), 87- 99.

Ocak, M.A. (2013). *Aile ve İnternet. Aile Eğitim Programı,* http://www.bildemkoleji.com/imgUp/files/AileVeInternet.pdf, Erişim Tarihi: 22.02.2022.

Odabaşı, H. F., Mısırlı, Ö., Günüç, S., Timar, Z., Ersoy, M., Som, S., Dönmez, F. İ., Akçay, O. ve Erol, O. (2012). Eğitim için yeni bir ortam: Twitter. *Anadolu Journal of Educational Sciences International (AJESI),* 2(1), 89-103.

Ohler, J. (2012). Digital citizenship means character education for the digital age. education digest: *Essential Readings Condensed for Quick Review*, 77(8), 14-17.

Onursoy, S. (2018). Üniversite gençliğinin dijital okuryazarlık düzeyleri: Anadolu Üniversitesi öğrencileri üzerine bir araştırma. *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi*, 6(2), 989-1013.

Orhon, N. (2019). *Medya Okuryazarlığı açısından Dijital Vatandaşlık Tartışmaları. Medya Okuryazarlığı Üzerine...* ed. Nilüfer Sezer, Nuray Yılmaz Sert. 1. bs. Konya: Eğitim.

Oyedemi, T. D. (2012). *The partially digital: İnternet, citizenship, social inequalities, and digital citizenship in South Africa*. Yayımlanmamış Doktora Tezi. Nigeria: ObafemıAwolowo University. https://scholarworks.umass.edu/dissertations/AAI3518402/, Erişim Tarihi: 11.02.2022.

Öğütçü, G., Testik, Ö. M., ve Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 56, 83- 93.

Öztürk, M. (2015). *Ortaokul Öğrencilerinin Dijital Vatandaşlık Düzeyleri*, (Yayımlanmamış Yüksek Lisans Tezi). Kastamonu Üniversitesi, Kastamonu.

Pamuk, S,, Çakır, R., Ergun, M., Yılmaz, H.B., Ayas, C. (2013). Öğretmen ve öğrenci bakış açısıyla tablet pc ve etkileşimli tahta kullanımı: FATİH projesi değerlendirmesi. *Kuram ve Uygulamada Eğitim Bilimleri,* 13(3), 1799-1822.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*, 66, 40-51.

Praveena, A., ve Smys, S. (2017, Nisan). Ensuring data security in cloud based social networks. *2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA),* RVS Technical Campus, Coimbatore. https://www.aconf.org/conf_89022.html., Erişim Tarihi: 23.02.2022.

Prensky, M. (2005). Listen to the natives. educational leadership. *Learning in the Digital Age*, 63 (4), 8-13.

Ribble, M. (2004). Digital citizenship: addressing appropriate technology behavior. *Learning and Leading With Technology*, 32(1), 6-11.

Ribble, M. (2011). Digital Citizenship in Schools. International Society for Technology in Education: Washington.

Ribble, M. (2015). *Digital Citizenship in Schools, Nine Elements All Students Should know.* (3rd ed.) Washington DC: International Society for Technology in Education.

Ribble, M. ve Bailey, G. (2007). *Digital Citizenship in Schools*. Washington, DC: ISTE

Sağır, M., Doğruluk, S., Mutluay, Y., ve Emlik, H. (2018). Meslek yüksekokulu öğrencilerinin bilgi güvenliği farkındalık düzeylerinin incelenmesi. *Akademik Sosyal Araştırmalar Dergisi*, 6(74), 566-582.

Sakallı, H. (2015). *Sınıf öğretmeni adaylarının dijital vatandaşlık düzeyleri ile siber zorbalık eğilimleri arasındaki ilişkinin incelenmesi* (Yüksek Lisans Tezi). Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü, Aydın.

Sakallı, H. ve Çiftçi, S. (2016). Sınıf öğretmeni adaylarının dijital vatandaşlık düzeyleri ile siber zorbalık eğilimleri arasındaki ilişkinin incelenmesi: Adnan Menderes Üniversitesi ö*rneği. Eğitim Teknolojisi Kuram ve Uygulama*, 6(2), 100-119.

Sarı, İ. ve Taşer, S. (2018). Türkiye'de dijital vatandaşlıkla ilgili yapılan yüksek lisans ve doktora tezlerinin incelenmesi. *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi,* 6, 1063-1069.

Searson, M., Hancock, M., Soheil, N. and Shepherd, G. (2015). Digital citizenship within global contexts. *Education and Information Technologies*, 20(4), 729-741.

SELMA, (2019). Hacking Online Hate: Building an Evidence Base for Educators. www.hackinghate.eu, Erişim Tarihi: 23.02.2022.

Semerci, A. (2019). Eğitim fakültesi öğrencileri ile diğer fakültelerdeki öğrencilerin siber güvenlik farkındalıklarının karşılaştırılması. *Akdeniz Eğitim Araştırmaları Dergisi,* 29, 138-156.

Simplilearn (2021). What is digital security: Overview, types, and applications explained. https://www.simplilearn.com/what-is-digital-security-article, Erişim Tarihi: 23.02.2022.

Solichin, A., ve Ramadhan, E. W. (2017, Ekim). Enhancing data security using DES-based cryptography and DCT-based steganography. *3rd International Conference*

on Science in Information Technology (ICSITech), Universitas Pendidikan Indonesia, Bandung. https://ieeexplore.ieee.org/xpl/conhome/8241142/proceeding. Erişim Tarihi: 23.02.2022.

Solmaz, M. (2020). *Öğretmen Adaylarının Siber Bilgi Güvenliği Farkındalıklarının ve Dijital Vatandaşlık Düzeylerinin Farklı Değişkenler Bakımından İncelenmesi*, Yüksek Lisans Tezi, Mersin Üniversitesi, Mersin.

Som Vural, S. ve Kurt, A. (2018). Üniversite öğrencilerinin bakış açısıyla dijital vatandaşlık göstergelerinin incelenmesi, *Eğitim Teknolojisi Kuram ve Uygulama,* 8 (1), 60-80. DOI: 10.17943/etku.317713.

Sorbring, E. (2014). Parents' concerns about their teenage children's İnternet use. *Journal of Family Issues,* 35(1), 75-96.

Sosyal Medya Okuryazarlığı, (2019). http://fcl.eun.org/sml4change, Erişim Tarihi: 23.02.2022.

Suppo, C. A. (2013). *Digital citizenship instruction in Pennsylvania public schools: School leaders expressed beliefs and current practices*, (Yayımlanmamış doktora tezi). Indiana University of Pennsylvania). https://eric.ed.gov/?id=ED553014, Erişim Tarihi: 11.02.2022.

Suson, R. L. (2019). Appropriating digital citizenship in the context of basic education. *İnternational Journal of Education, Learning and Development,* 7 (4), 44-66.

Şahin, M. C. (2009). Yeni binyılın öğrencilerinin özellikleri. *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, 9(2), 155-172.

Şen, Ş., ve Yerlikaya, T., 2013. ISO 27001 Kurumsal Bilgi Güvenliği Standardı. Akademik Bilişim 2013 – *XV. Akademik Bilişim Konferansı Bildirileri*, 23-25 Ocak 2013 Antalya: Akdeniz Üniversitesi, 719-723.

Şener, G. ve Erdikmen, A. (2019) "*Yeni Medya Çalışmaları V: Türkiye İnternet Tarihi", iç. Türkiye'de Erken Dönem İnternet Aktivizmi*, (Ed.) Erkan Saka, İstanbul: Alternatif Bilişim Derneği.

Şimsek, E., ve Şimsek, A. (2013). New literacies for digital citizenship. *Contemporary Educational Technology,* 4 (2), 126-137.

Taha, N., ve Dahabiyeh, L. (2021). College students information security awareness: a comparison between smartphones and computers. *Education and Information Technologies*, 26(2), 1721-1736.

Talan, T., ve Aktürk C. (2021). Ortaöğretim öğrencilerinin dijital okuryazarlık ve bilgi güvenliği farkındalığı seviyelerinin incelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi,* 18(1), 158-180. https://doi.org/10.33437/ksusbd.668255.

Taner, E. ve Kılıç, İ. (2019). Güvenlik güçlerinin bilgi güvenliği farkındalığını belirlemeye yönelik bir araştırma. *Güvenlik Bilimleri Dergisi*, 8 (2), 253- 269.

Tatlı, A. (2018). *Öğretmenlerin Dijital Vatandaşlık Düzeylerinin Bilgi Okuryazarlığı ile İnternet ve Bilgisayar Kullanım Özyeterlilikleri bağlamında değerlendirilmesi*, (Yayımlanmamış Yüksek Lisans Tezi). Necmettin Erbakan Üniversitesi, Konya.

TBMM, (2020). "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun", https://www.tbmm.gov.tr/kanunlar/k7253.html, Erişim Tarihi: 26.02.2022.

Tekerek, M. ve Tekerek, A. (2013). Öğrencilerin bilgi güvenliği farkındalığı üzerine bir araştırma. *Turkish Journal of Education*. 2(3). 61-70. https://doi.org/10.19128/turje.181065.

Telli, E. (2020). Dijital Erişim, A.A. Kurt ve F. Odabaşı (Ed.) *Pandemi Döneminde Sınanan Dijital Vatandaşlık içinde* (57-86). Ankara: Anı.

Teo, T., Kabakçı Yurdakul, I., ve Ursavaş, Ö. F. (2014). Exploring the digital natives among pre-service teachers in Turkey: a cross-cultural validation of the digital native assessment scale. *Interactive Learning Environments, (ahead-of-print*), 1-14.

Timur, B., Timur, S., & Akkoyunlu, B. (2014). Öğretmen adaylarının sayısal yetkinlik düzeylerinin belirlenmesi. *Muğla Sıtkı Koçman Üniversitesi Sosyal ve Beşerî Bilimler Araştırmaları Dergisi,* (33), 41-59.

Tsohou, A., Karyda, M., ve Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. *Computers & Security*, 52, 128-141.

TÜİK, (2021). https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2021-37437, Erişim Tarihi: 20.02.2022.

Türkiye Cumhuriyeti Anayasası, (1982). https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5#:~:text=Madde%2020%20%E2%80%93%20Herkes%2C%20%C3%B6zel%20hayat%C4%B1na,%2D4709%2F5%20md.), Erişim Tarihi: 25.02.2022.

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J. and Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, 75(1), 547-559.

Vigderman, A. ve Turner, G. (2021). A 2021 Guide to personal digital security & online safety. https://www.security.org/digital-safety/, Erişim Tarihi: 24.02.2022.

Winn, M. R. (2012). Promote digital citizenship through school-based social Networking. *Learning and Leading with Technology*, 39(4), 10-13.

Wisniewski, P., Xu, H., Rosson, M. B., ve Carroll, J. M. (2017). Parents Just Don't Understand: Why Teens Don't Talk to Parents about Their Online Risk Experiences. In Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (pp. 523-540). ACM.

Yalçınkaya, B. ve Cibaroğlu, M. O. (2019). Dijital vatandaşlık algısının incelenmesi: ampirik bir değerlendirme. *Business & Management Studies: An İnternational Journal*, 7(4), 1188-1208.

Yapar, N.N. (2019). Google Türkiye ve BTK'dan Ortak Proje: "İnternot Olmaya Var mısın?". https://dijitalmedyavecocuk.bilgi.edu.tr/2019/04/19/google-turkiye-ve-btkdan-ortak-proje-internot-olmaya-var-misin/, Erişim Tarihi: 22.02.2022.

Yılmaz, E., Şahin, Y. L. ve Akbulut, Y. (2015). Dijital veri güvenliği farkındalığı ölçeğinin geliştirilmesi. AJIT-e: Online Academic Journal of Information Technology, 6(21), 23-40

Yılmaz, E., Şahin, Y., ve Akbulut, Y., (2016). Öğretmenlerin dijital veri güvenliği farkındalığı, *Sakarya University Journal Of Education*, 6, (2)26-45.

Yılmaz, M. (2019). *Öğretmen adaylarının dijital vatandaşlık düzeylerinin belirlenmesi: Mersin Üniversitesi Eğitim Fakültesi örneği*. Yayımlanmamış Yüksek Lisans Tezi, Mersin Üniversitesi. Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı, Mersin.

Yılmaz, M., ve Doğusoy, B. (2020). Öğretmen adaylarının dijital vatandaşlık düzeylerinin belirlenmesi, *Kastamonu Education Journal*, 28 (6): 2362-2375 doi: 10.24106/kefdergi.692492.

EKLER

EK 1: Kişisel Bilgi Soruları

Sayın öğrenci;
Aşağıdaki sorular "Üniversite Öğrencilerinin Dijital Veri Güvenliği Farkındalıklarının Dijital Vatandaşlık Bağlamında İncelenmesi" başlıklı yüksek lisans tezim için hazırlanmıştır. Kimliğinizi belli edecek özel hiçbir soru sorulmadığından yanıtların kimden geldiği bilinmeyecektir. Araştırmaya katılmak tamamen gönüllülük esasına dayanmaktadır. Vereceğiniz yanıtlar sadece bu tez çalışmasında kullanılacaktır. Tezime verdiğiniz değerli destek için teşekkür eder, derslerinizde başarılar dilerim.

Mert Hızmalı (Yüksek lisans öğrencisi)
merthizmali@ogr.trakya.edu.tr

1. Cinsiyetiniz:
   () Erkek
   () Kadın
2. Öğrenim görmekte olduğunuz eğitim kademesi:
   () Ön lisans
   () Lisans
   () Yüksek Lisans/Doktora
3. Sınıfınız (*Rakamla yazınız*): …….
4. Günlük ortalama internet kullanma (*Eğitsel, eğlence, sosyal ağlarda iletişim, e-posta işlemleri gibi amaçlarla*) süreniz kaç saattir?
   () Kullanmıyorum
   () 0 -1
   () 2-3
   () 4-5
   () 6-7
   () 8 ve üzeri
5. Hangi teknolojik cihazlara sahipsiniz? (*Birden çok seçenek işaretleyebilirsiniz.)*
   () Akıllı telefon
   () Dizüstü bilgisayar
   () Tablet
   () Masaüstü bilgisayar
   () Smart tv
   () Hiçbirine sahip değilim
6. Ailenizin aylık ortalama gelir düzeyi nedir?
   () 7501-10000
   () 5001-7500
   () 5000 ve altı

() 10000 üzeri

7. Üniversitenizde öğrencilerin dijital vatandaşlık hakkında farkındalık ve bilgi sahibi olmaları için üniversite yönetiminden ne tür beklentileriniz bulunmaktadır?
8. Üniversitenizde öğrencilerin dijital veri güvenliği konusunda farkındalık ve bilgi sahibi olmaları için üniversite yönetiminden ne tür beklentileriniz bulunmaktadır?

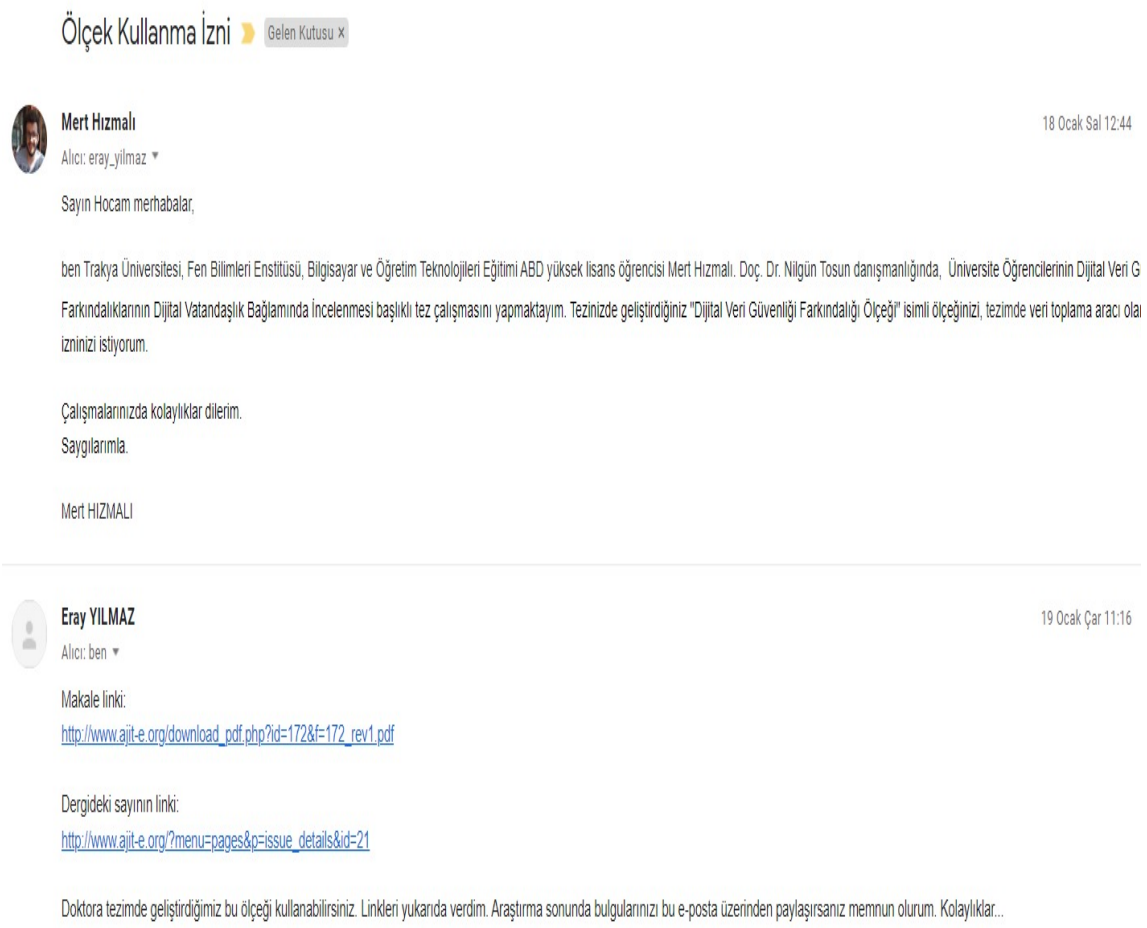
EK 2: Dijital Vatandaşlık Ölçeği

ÖLÇEK MADDELERİ	Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılmıyorum
Dijital ortamlarda yapılan yardım çağrılarına destek veririm.					
Dijital araçları bu araçlardan kaynaklanabilecek sağlık sorunlarına (göz/iskelet sistemi rahatsızlıkları vb.) dikkat ederek kullanırım.					
Dijital araçları kullanırken çalışma ortamı ergonomik (rahat, kullanımı kolay) açıdan uygun şekilde (masa, sandalye, ortam ışığı vb.) düzenlerim.					
Dijital ortamlara (sosyal ağlar, haber siteleri, bloglar vb.) çeşitli dijital araçlarla istediğim an bağlanırım.					
Güvenliğinden emin olmadığım dijital araçlarla parola gerektiren işlemleri yapmam.					
Haberleşme amaçlı farklı dijital iletişim ortamları (eposta, sosyal paylaşım siteleri, bloglar, WhatsApp vb.) kullanırım.					
Çevrimiçi alışveriş yapmadan önce ürün veya hizmet ile ilgili bir araştırma (fiyat, kalite vb.) yaparım.					
Dijital ortamlara pek çok yerden (okul, ev vb.) bağlanırım.					
Dijital ortamlardaki toplumsal sorumluluk projelerine katılımda bulunurum.					

Dijital ortamlarda ürün veya hizmet satın alırım.					
Dijital ortamlardaki paylaşımların bireyler üzerindeki etkisinin farkındayım.					
Dijital araçları kullanarak resmi işlemlerimi (bankacılık işlemleri, nüfus, askerlik, ikametgâh vb.) yürütürüm					
Dijital ortamlarda gizlilik ayarlarını düzenlerim.					
Kaynağından emin olmadığım e-posta ve iletileri açmam.					
Dijital ortamlarda önemli kimlik bilgilerimi paylaşmam.					
Kitlesel suç (toplumu örgütleme, hakaret etme vb.) işlenebilecek dijital ortamlarda bulunmam.					
Gerektiğinde alışveriş sitelerinden aldığım ürünlerin iade veya değişimini yaparım.					
Dijital ortamlarda sahip olduğum parolalarımı kimseyle paylaşmam.					
Dijital ortamlarda doğruluğundan emin olmadığım bilgileri paylaşmam.					
Dijital ortamlarda fark edilen sahte kullanıcılar konusunda çevremdekileri uyarırım.					
Güvenliğinden emin olmadığım web sayfalarına üye olmam.					
Dijital araçları kullanırken göz					

sağlığım için uygun ekran ayarlarını (parlaklık, boyut vb.) yaparım.					
Dijital ortamlarda iletişime geçmem ya da geçmememem gereken kişileri ayırt ederim.					

EK 3: Dijital Vatandaşlık Ölçek Kullanım İzni



Ölçek Kullanma İzni Gelen Kutusu ×

Mert Hızmalı 18 Ocak Sal 12:44

Alıcı: eray_yilmaz

Sayın Hocam merhabalar,

ben Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar ve Öğretim Teknolojileri Eğitimi ABD yüksek lisans öğrencisi Mert Hızmalı. Doç. Dr. Nilgün Tosun danışmanlığında, Üniversite Öğrencilerinin Dijital Veri G Farkındalıklarının Dijital Vatandaşlık Bağlamında İncelenmesi başlıklı tez çalışmasını yapmaktayım. Tezinizde geliştirdiğiniz "Dijital Veri Güvenliği Farkındalığı Ölçeği" isimli ölçeğinizi, tezimde veri toplama aracı olar izninizi istiyorum.

Çalışmalarınızda kolaylıklar dilerim.
Saygılarımla.

Mert HIZMALI

Eray YILMAZ 19 Ocak Çar 11:16

Alıcı: ben

Makale linki:
http://www.ajit-e.org/download_pdf.php?id=172&f=172_rev1.pdf

Dergideki sayının linki:
http://www.ajit-e.org/?menu=pages&p=issue_details&id=21

Doktora tezimde geliştirdiğimiz bu ölçeği kullanabilirsiniz. Linkleri yukarıda verdim. Araştırma sonunda bulgularınızı bu e-posta üzerinden paylaşırsanız memnun olurum. Kolaylıklar...

EK 4: Dijital Veri Güvenliği Ölçeği

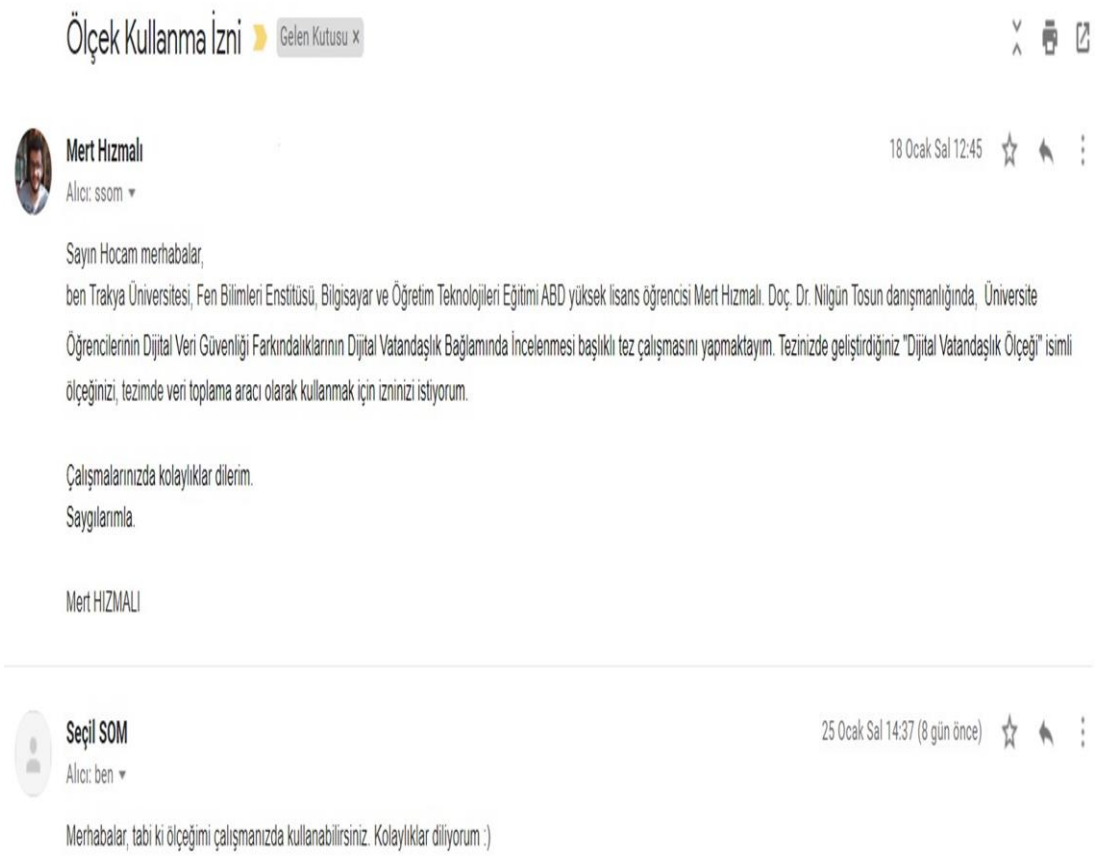
ÖLÇEK MADDELERİ	Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılmıyorum
Zararlı yazılımlar (virüs, solucan, truva atı vb.) konusunda bilgi sahibiyim.					
Parola oluştururken harf, sayı ve özel karakter kullanmanın önemini bilirim.					

Farklı işlemler için farklı parola kullanmanın önemini bilirim.					
İzinsiz kullanılmaması için dosyalara parola konulabileceğinin farkındayım.					
Güvenlik duvarı yazılımları konusunda bilgi sahibiyim.					
Flash bellekleri, veri saklamak yerine sadece veri taşımak için kullanmanın farkını bilirim.					
İşletim sisteminin (Windows, Android vb.) güncel olmasına dikkat ederim.					
E-posta ile gelen kimlik bilgilerini doğrulama mesajlarına (parola, kredi kartı vb.) itibar edilmemesi gerektiğini bilirim.					
Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) kullanmadan önce virüs taraması yapılması gerektiğini bilirim.					
Güvenli olmadığını düşündüğüm e-postaları açmadan silmeye dikkat ederim.					
Programların, üreticinin kendi sitesinden indirilmesinin önemini bilirim.					
Antivirüs yazılımı kullanmanın önemini bilirim.					
Parola hatırlatmak için kullanılan güvenlik sorularına başkalarının tahmin edemeyeceği cevaplar verilmesi gerektiğini bilirim.					
Parola oluştururken karakter sayısının fazla olmasının önemini bilirim.					
Parolaların herhangi bir ortamda saklanmasının güvenlik riski oluşturacağının farkındayım.					

Verilerin, çeşitli uygulamalar (Dropbox, Google Drive vb.) kullanılarak İnternet ortamında saklanabileceğini bilirim.					
Üzerinde çalışma yapılan dosyaların birden fazla ortamda yedeklenmesi gerektiğini bilirim.					
Başkalarının tahmin edemeyeceği parolalar oluşturmaya dikkat ederim.					
İnternet adres çubuğunda yanlış yönlendirme olup olmadığına dikkat ederim					
Taşınabilir depolama birimlerini (Flash bellek, taşınabilir sabit disk) "Donanımı Güvenle Kaldır" seçeneğini kullanarak çıkartmaya dikkat ederim.					
Karmaşık yapıdaki parolaların kırılabileceğini bilirim.					
Parolaların belirli aralıklarla değiştirilmesi gerektiğinin farkındayım.					
Almak istemediğim çöp e-postaları "spam/gereksiz/önemsiz" olarak işaretlemeye dikkat ederim.					
İzinsiz kullanılmaması için cihazlara (akıllı telefon, tablet, bilgisayar vb.) parola konulabileceğinin farkındayım.					
Kendime ait olmayan cihazlarda, parola gerektiren işlemler yapmamaya dikkat ederim.					
İşletim sisteminin (Windows, Android vb.) güvenlikle ilgili uyarılarını dikkate alırım					
Elektrik kesintisine karşı dizüstü bilgisayarları bataryası ile kullanmanın önemini bilirim.					
Cep telefonuna gelen tek kullanımlık parola ile yapılan giriş işlemlerinin,					

güvenliği arttırdığını bilirim.					
Sanal klavye kullanmanın önemini bilirim.					
İnternet sitelerinde kullanıcı oturumunu kapatırken "güvenli çıkış" bağlantısını kullanmanın önemini bilirim.					
İnternet sitelerinde kullanılan güvenlik sertifikaları hakkında bilgi sahibiyim.					
Lisanslı olmayan yazılımların güvenlik açıkları oluşturabileceğinin farkındayım					

EK 5: Dijital Veri Güvenliği Ölçek Kullanım İzni



Ölçek Kullanma İzni Gelen Kutusu x

Mert Hızmalı 18 Ocak Sal 12:45

Alıcı: ssom

Sayın Hocam merhabalar,

ben Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar ve Öğretim Teknolojileri Eğitimi ABD yüksek lisans öğrencisi Mert Hızmalı. Doç. Dr. Nilgün Tosun danışmanlığında, Üniversite Öğrencilerinin Dijital Veri Güvenliği Farkındalıklarının Dijital Vatandaşlık Bağlamında İncelenmesi başlıklı tez çalışmasını yapmaktayım. Tezinizde geliştirdiğiniz "Dijital Vatandaşlık Ölçeği" isimli ölçeğinizi, tezimde veri toplama aracı olarak kullanmak için izninizi istiyorum.

Çalışmalarınızda kolaylıklar dilerim.

Saygılarımla.

Mert HIZMALI

Seçil SOM 25 Ocak Sal 14:37 (8 gün önce)

Alıcı: ben

Merhabalar, tabi ki ölçeğimi çalışmanızda kullanabilirsiniz. Kolaylıklar diliyorum :)

EK 6: Etik Kurul Onayı

Evrak Tarih Sayısı: 01.03.2022-218377

T.C.
TRAKYA ÜNİVERSİTESİ REKTÖRLÜĞÜ
Sosyal ve Beşeri Bilimler Araştırmaları Etik Kurulu Başkanlığı

Sayı : E-29563864-050.04.04-218377 01.03.2022
Konu : Kararlar

Sayın Doç. Dr. Nilgün TOSUN

Danışmanlığını yaptığınız, Trakya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Yüksek Lisans Programı öğrencisi Mert HIZMALI tarafından yapılmış olunan başvuru, Trakya Üniversitesi Sosyal ve Beşeri Bilimler Araştırmaları Etik Kurulu'nun 23.02.2022 tarihli toplantısında alınan 02/07 numaralı kararı ile uygun görülmüştür.

Gereğini bilgilerinize rica ederim.

Prof. Dr. Ayhan GENÇLER
Başkan

Ek:Etik Kurul Kararı

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Belge Doğrulama Kodu :BSN60EHAAF Pin Kodu :18062 Belge Takip Adresi : https://www.turkiye.gov.tr/trakya-universitesi-ebys

Doç. Dr. Esma MIHLAYANLAR
Üye
Mimarlık Fakültesi
Araştırma ile ilişkisi ☐var ☒yok
Toplantı Katılım ☒evet ☐hayır

Doç.Dr. Ahmet Emre DAĞTAŞOĞLU
Üye
İlahiyat Fakültesi
Araştırma ile ilişkisi ☐var ☒yok
Toplantı Katılım ☒evet ☐hayır

Doç. Dr. Emre ATILGAN
Üye
Proje Koordinasyon Uyg.ve Arş.Merk
Araştırma ile ilişkisi ☐var ☐yok
Toplantı Katılım ☐evet ☒hayır

Dr. Öğr. Üyesi Levent DOĞAN
Üye
Sosyal Bilimler Enstitüsü
Araştırma ile ilişkisi ☐var ☒yok
Toplantı Katılım ☒evet ☐hayır

Dr. Öğr. Üyesi Ayşegül KILIÇ
Üye
Balkan Araştırma Enstitüsü
Araştırma ile ilişkisi ☐var ☒yok
Toplantı Katılım ☒evet ☐hayır

Doç. Dr. Esma MIHLAYANLAR
Üye
Mimarlık Fakültesi
Araştırma ile ilişkisi ☐var ☒yok
Toplantı Katılım ☒Evet ☐hayır

Doç.Dr. Ahmet Emre DAĞTAŞOĞLU
Üye
İlahiyat Fakültesi
Araştırma ile ilişkisi ☐var ☒yok
Toplantı Katılım ☒Evet ☐hayır

Doç. Dr. Emre ATILGAN
Üye
Proje Koordinasyon Uyg.ve Arş.Merk
Araştırma ile ilişkisi ☐var ☐yok
Toplantı Katılım ☐Evet ☒hayır

Dr. Öğr. Üyesi Levent DOĞAN
Üye
Sosyal Bilimler Enstitüsü
Araştırma ile ilişkisi ☐var ☒yok
Toplantı Katılım ☒Evet ☐hayır

Dr. Öğr. Üyesi Ayşegül KILIÇ
Üye
Balkan Araştırma Enstitüsü
Araştırma ile ilişkisi ☐var ☒yok
Toplantı Katılım ☒Evet ☐hayır

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı: Mert HIZMALI

Eğitim

Derece	**Eğitim Birimi**	**Bölüm**	**Mezuniyet Tarihi**
Yüksek Lisans	T.Ü. Fen Bilimleri Enstitüsü	BÖTE	2022
Lisans	T.Ü. Eğitim Fakültesi	Bilgisayar Öğretmenliği	2020
Lisans	A.Ü. İktisat Fakültesi	Uluslararası İlişkiler	2022
Lise	Emel Özgür Subaşıay A.L.	Bilişim Teknolojileri	2016

İş Deneyimi

Yıl	**Yer**	**Görev**
2014-2016	Edirne	Editör- Haber Editörü
2016-2016	Edirne	Bilgi İşlem Stajyeri
2017-2018	Edirne	Editör
2019- ……	Edirne	Yönetim Müdürü
2019- ……	Edirne	Yazılım ve Kodlama Eğitmeni

Yabancı Dil

İngilizce	İyi derece
Rusça	Başlangıç
Korece	Başlangıç